PROGRAM FUNKCJONALNO-UŻYTKOWY

ROZBUDOWA SYSTEMU RIS NA ODRZAŃSKIEJ DRODZE WODNEJ

Fundusze Europejskie na Infrastrukturę, Klimat, Środowisko
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Projekt współfinansowany przez Unię Europejską ze środków Funduszu Spójności w ramach

Programu Fundusze Europejskie na Infrastrukturę, Klimat, Środowisko 2021-2027

PROGRAM FUNKCJONALNO – UŻYTKOWY

„ROZBUDOWA SYSTEMU RIS NA ODRZAŃSKIEJ DRODZE WODNEJ”

FENX.04.04-IP.02-0001/24

Zamawiający:

Urząd Żeglugi Śródlądowej w Szczecinie

SZCZECIN, 2026

Nazwa zamówienia:

Rozbudowa systemu RIS na Odrzańskiej Drodze Wodnej

Zakres Projektu:

Projekt obejmuje rozbudowę systemu RIS na Odrzańskiej Drodze Wodnej (ODW) poprzez rozszerzenie infrastruktury radiokomunikacyjnej VHF/AIS, monitoringu wizyjnego CCTV, czujników hydrologicznych i meteorologicznych, sieci transmisji danych oraz zaplecza serwerowego Centrum RIS. Zakres przedsięwzięcia obejmuje również modernizację wybranych elementów istniejącego systemu RIS na Odrzańskiej Drodze Wodnej oraz wdrożenie usług cyfrowych, usług VTT i informacji hydrometeorologicznej. Celem projektu jest zwiększenie obszaru objętego usługami RIS, poprawa dostępności informacji żeglugowej oraz wsparcie bezpieczeństwa i efektywności żeglugi śródlądowej na ODW.

Nazwa Zamawiającego:

Urząd Żeglugi Śródlądowej w Szczecinie

Pl. Batorego 4

70-207 Szczecin

Autorzy opracowania:

Praca zespołowa wykonana przez zespół specjalistów w składzie:

FXGRAIL Sp. z o. o.
ul. Złota 61
00-890 Warszawa

IdeaConcept Jacek Hawrylczak
ul. Powstańców Warszawy 1 lok. 14
65-807 Zielona Góra

Zawartość Programu Funkcjonalno-Użytkowego:

1. Część opisowa:

1.1. Opis ogólny przedmiotu zamówienia

1.2. Opis wymagań Zamawiającego w stosunku do przedmiotu zamówienia

2. Część informacyjna

Spis Treści

SPIS TREŚCI ... **3**

STRESZCZENIE ... **10**

ABSTRACT ... **12**

1. CZĘŚĆ OPISOWA ... **15**

1.1. OPIS OGÓLNY PRZEDMIOTU ZAMÓWIENIA ... 15

1.1.1. Generalne założenia projektu rozbudowy RIS na ODW ... *16*

1.1.1.1. Cel, tło i logika interwencji ... 17

1.1.1.2. Analiza stanu istniejącego i doświadczeń z wcześniejszych wdrożeń ... 17

1.1.1.3. Zakres terytorialny ... 18

1.1.1.4. Zakres rzeczowy inwestycji ... 20

1.1.1.5. Miejsce realizacji przedmiotu zamówienia ... 21

1.1.1.5.1. Obiekty wieżowe stacji radiokomunikacyjnych VHF/AIS, czujników meteorologicznych oraz kamer monitoringu wizyjnego ... 21

1.1.1.5.2. Punkty monitoringu wizyjnego oraz stacji czujników hydrologicznych ... 23

1.1.1.5.3. Obiekty wymiany obecnych urządzeń i elementów systemu RIS ... 25

1.1.1.5.4. Obiekty hydrotechniczne monitorowane na bazie infrastruktury RZGW ... 37

1.1.1.5.5. Zbiorcze zestawienie nowych lokalizacji terenowych oraz ich funkcji ... 38

1.1.2. Opis rozbudowy i modernizacji systemu RIS ... *41*

1.1.2.1. Rozbudowa systemu łączności radiowej VHF/AIS/DGNSS ... 41

1.1.2.2. Rozbudowa i modernizacja systemu monitoringu wizyjnego (CCTV) ... 44

1.1.2.3. Rozbudowa sieci transmisji danych ... 46

1.1.2.4. Czujniki hydrologiczne (wodowskazy) ... 49

1.1.2.5. Sensory meteorologiczne ... 50

1.1.2.6. Wieże, maszty, konstrukcje wsporcze i infrastruktura teletechniczna ... 52

1.1.2.7. Doposażenie serwerowni głównej systemu RIS ... 54

1.1.2.8. Modernizacja pomieszczenia serwerowni pełniącej rolę węzła telekomunikacyjnego ... 55

1.1.2.9. Modernizacja sieci teleinformatycznej ... 57

1.1.2.10. Środowisko pracy zmodernizowanego systemu RIS ... 59

1.1.2.11. Utworzenie serwerowni zapasowej oraz łącza teleinformatycznego łączącego ją z Centrum RIS ... 63

1.1.2.12. Usługi cyfrowe RIS ... 65

1.1.2.13. Monitoring techniczny zasobów infrastrukturalnych i aplikacyjnych systemu ... 67

1.2. OPIS WYMAGAŃ ZAMAWIAJĄCEGO W STOSUNKU DO PRZEDMIOTU ZAMÓWIENIA ... 71

1.2.1. Wymagania w stosunku do zgodności prawnej i normatywnej ... *72*

1.2.1.1. Klauzula ogólna zgodności prawnej i normatywnej ... 73

1.2.1.2. Wymagania wynikające z prawa Unii Europejskiej i standardów RIS ... 74

1.2.1.3. Wymagania wynikające z polskich przepisów dotyczących RIS, żeglugi śródlądowej i dróg wodnych ... 75

1.2.1.4. Wymagania dotyczące zamówień publicznych, dokumentacji projektowej ... 76

1.2.1.5. Wymagania budowlane, lokalizacyjne i infrastrukturalne ... 77

1.2.1.6. Wymagania środowiskowe, wodnoprawne, odpadowe i PEM ... 79

1.2.1.7. Wymagania dotyczące łączności elektronicznej, radiokomunikacji i zgodności urządzeń ... 80

1.2.1.8. Wymagania dotyczące cyberbezpieczeństwa, danych, usług cyfrowych i dostępności ... 81

1.2.1.9. Wymagania wynikające z finansowania, polityk horyzontalnych i oznakowania projektu ... 82

1.2.1.10. Wymagania normatywne i standardy techniczne dla usług RIS ... 83

1.2.1.11. Wymagania normatywne dla VHF, AIS, DGNSS i infrastruktury antenowej ... 83

1.2.1.12. Wymagania normatywne dla systemu monitoringu wizyjnego CCTV/VSS ... 84

1.2.1.13. Wymagania normatywne dla sieci transmisyjnej, VPN i infrastruktury IP ... 85

1.2.1.14. Wymagania normatywne dla serwerowni, infrastruktury serwerowej i ciągłości działania ... 85

1.2.1.15. Wymagania normatywne dla konstrukcji, posadowienia i ochrony antykorozyjnej ... 86

1.2.1.16. Wymagania normatywne dla zasilania, ochrony odgromowej, uziemień i ochrony przepięciowej ... 87

1.2.1.17. Wymagania normatywne dla cyberbezpieczeństwa, jakości oprogramowania i testów ... 87

1.2.1.18. Wymagania dotyczące dokumentów zgodności, odbiorów i przekazania do eksploatacji ... 88

1.2.1.19. Wymagania dotyczące aktualizacji wykazu przepisów i norm w toku realizacji ... 89

1.2.2. Zasady projektowania 89
1.2.3. Wymagania w stosunku do systemu łączności radiowej VHF/AIS/DGNSS 96
1.2.4. Wymagania w stosunku do systemu monitoringu wizyjnego (CCTV) 98
1.2.5. Wymagania w stosunku do sieci połączeń transmisyjnych 100
1.2.6. Wymagania dla czujników hydrologicznych i danych pomiarowych 102
1.2.7. Wymagania dla czujników meteorologicznych i danych pomiarowych 108
1.2.8. Wymagania dla wież, masztów, konstrukcji wsporczych i terenowej infrastruktury teletechnicznej 114
1.2.8.1. Wymagania techniczne dla obiektów wieżowych stacji radiokomunikacyjnych 116
1.2.8.1.1. Wysokość i geometria wieży 116
1.2.8.1.2. Konstrukcja stalowa i zabezpieczenie antykorozyjne 117
1.2.8.1.3. Fundament i warunki posadowienia 117
1.2.8.1.4. Platforma techniczna 118
1.2.8.1.5. Drabina wewnętrzna i komunikacja pionowa 119
1.2.8.1.6. System asekuracyjny 119
1.2.8.1.7. System prowadzenia torów antenowych i okablowania 120
1.2.8.1.8. Konstrukcje wsporcze dla anten, sensorów i urządzeń 121
1.2.8.1.9. Ochrona odgromowa, uziemienie i połączenia wyrównawcze 122
1.2.8.1.10. Oznakowanie przeszkodowe i malowanie przeszkodowe 122
1.2.8.1.11. Ogrodzenie i zabezpieczenie terenu 123
1.2.8.1.12. Szafa teletechniczna i powiązanie z wieżą 123
1.2.8.1.13. Tablice informacyjne i oznakowanie projektu 123
1.2.8.1.14. Wymagania formalne i projektowe 124
1.2.8.1.15. Wymagania odbiorowe 125
1.2.8.1.16. Przeglądy techniczne, kontrole okresowe i utrzymanie wież w okresie realizacji oraz gwarancji 125
1.2.8.2. Wymagania techniczne dla słupa kamerowego o wysokości 6 m 127
1.2.8.3. Wymagania techniczne dla szaf teletechnicznych typu zewnętrznego 131
1.2.8.4. Wymagania techniczne dla konstrukcji wsporczych 139
1.2.9. Wymagania dla nowych zasilaczy awaryjnych oraz wymiany zasilaczy awaryjnych lub zasobników energii 145
1.2.9.1. Opis wymagań dla zasilacza awaryjnego 147
1.2.9.2. Opis wymagań dla wymiany modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA 150
1.2.10. Wymagania dla modernizacji serwerowni 152
1.2.10.1. Przedmiot zadania 152
1.2.10.2. Stan istniejący i docelowy układ pomieszczenia 152
1.2.10.3. Zakres odpowiedzialności Generalnego Wykonawcy 154
1.2.10.4. Wymagania dotyczące dokumentacji projektowej 154
1.2.10.5. Wymagania dotyczące ciągłości działania podczas realizacji prac 155
1.2.10.6. Wymagania budowlano-adaptacyjne 156
1.2.10.7. Drzwi, zabezpieczenia fizyczne i dostęp do pomieszczenia 157
1.2.10.8. Zasilanie serwerowni telekomunikacyjnej 158
1.2.10.9. Dedykowany kanał kablowy dla toru zasilającego 158
1.2.10.10. Szafy RACK i organizacja zabudowy technicznej 160
1.2.10.11. Klimatyzacja pomieszczenia oraz system precyzyjnego chłodzenia szaf RACK 161
1.2.10.12. Trasy kablowe i okablowanie wewnętrzne 163
1.2.10.13. Kontrola dostępu 164
1.2.10.14. System ochrony przeciwpożarowej i gaszenia 165
1.2.10.15. Monitoring techniczny i zarządzanie infrastrukturą 165
1.2.10.16. Wymagania dotyczące urządzeń aktywnych i infrastruktury LAN 166
1.2.10.17. Wymagania dotyczące bezpieczeństwa i separacji 168
1.2.10.18. Testy, pomiary i odbiór 168
1.2.10.19. Dokumentacja powykonawcza i eksploatacyjna 169
1.2.10.20. Rezultat końcowy 170
1.2.11. Wymagania dla modernizacji sieci teleinformatycznej 170
1.2.11.1. Przedmiot zadania 170
1.2.11.2. Zakres lokalizacyjny 171
1.2.11.3. Zakres rzeczowy modernizacji 171

1.2.11.4. Wymagania dotyczące dokumentacji projektowej ... 172
1.2.11.5. Zasady prowadzenia tras kablowych ... 173
1.2.11.6. Prowadzenie tras kablowych w pomieszczeniach ... 174
1.2.11.7. Separacja instalacji sygnałowych i zasilających ... 175
1.2.11.8. Punkty elektryczno-logiczne PEL ... 175
1.2.11.9. Punkty logiczne RJ45 PoE dla tabletów informacyjnych ... 176
1.2.11.10. Minimalny zakres ilościowy punktów ... 176
1.2.11.11. Okablowanie strukturalne ... 177
1.2.11.12. Punkty koncentracji sieci ... 177
1.2.11.13. Przełączniki dostępowe PoE ... 178
1.2.11.14. Zasilanie punktów PEL i urządzeń sieciowych ... 178
1.2.11.15. Wymagania dotyczące zabytkowego charakteru budynku i estetyki wykonania ... 179
1.2.11.16. Organizacja prac i minimalizacja uciążliwości ... 180
1.2.11.17. Oznakowanie i administracja instalacją ... 180
1.2.11.18. Testy, pomiary i odbiór ... 181
1.2.11.19. Dokumentacja powykonawcza ... 181
1.2.11.20. Rezultat końcowy ... 182
1.2.12. Wymagania dla doposażenia serwerowni głównej ... 183
1.2.12.1. Wymagania dotyczące rozbudowy kart sieciowych w serwerach kasetowych Dell EMC PowerEdge MX740c 184
1.2.12.1.1. Przedmiot zadania ... 184
1.2.12.1.2. Stan istniejący środowiska ... 184
1.2.12.1.3. Zakres serwerów objętych modernizacją ... 185
1.2.12.1.4. Wymagania dotyczące dostarczanych kart sieciowych ... 185
1.2.12.1.5. Wymagania instalacyjne ... 186
1.2.12.1.6. Wymagania konfiguracyjne ... 187
1.2.12.1.7. Wymagania dotyczące wysokiej dostępności ... 187
1.2.12.1.8. Wymagania dotyczące testów i odbioru ... 188
1.2.12.1.9. Wymagania dotyczące dokumentacji ... 189
1.2.12.1.10. Wymagania dotyczące gwarancji i wsparcia ... 189
1.2.12.1.11. Wymagania dotyczące realizacji prac w środowisku produkcyjnym ... 189
1.2.12.1.12. Rezultat końcowy ... 190
1.2.12.2. Wymagania dotyczące rozbudowy macierzy dyskowej Dell EMC PowerVault ME4024 ... 190
1.2.12.2.1. Przedmiot zadania ... 190
1.2.12.2.2. Stan istniejący ... 191
1.2.12.2.3. Wymagany zakres dostawy ... 191
1.2.12.2.4. Wymagania dla półki dyskowej ... 191
1.2.12.2.5. Wymagania dla dysków SSD ... 192
1.2.12.2.6. Wymagania dotyczące konfiguracji pojemności ... 193
1.2.12.2.7. Wymagania dotyczące integracji z VMware vSphere ... 193
1.2.12.2.8. Wymagania dotyczące iSCSI i sieci storage ... 194
1.2.12.2.9. Wymagania instalacyjne ... 194
1.2.12.2.10. Wymagania dotyczące bezpieczeństwa danych ... 195
1.2.12.2.11. Wymagania dotyczące testów odbiorowych ... 195
1.2.12.2.12. Wymagania dotyczące dokumentacji powykonawczej ... 196
1.2.12.2.13. Wymagania dotyczące gwarancji i wsparcia ... 196
1.2.12.2.14. Rezultat końcowy ... 197
1.2.12.3. Wymagania dotyczące rozbudowy rozwiązania Dell EMC Avamar DP4400 / Integrated Data Protection Appliance / PowerProtect DP4400 ... 197
1.2.12.3.1. Przedmiot zadania ... 197
1.2.12.3.2. Cel rozbudowy ... 197
1.2.12.3.3. Weryfikacja stanu istniejącego ... 198
1.2.12.3.4. Wymagania dotyczące dostawy ... 198
1.2.12.3.5. Wymagania dotyczące licencji ... 199
1.2.12.3.6. Wymagania dotyczące wykonania rozbudowy ... 199
1.2.12.3.7. Wymagania dotyczące ciągłości działania ... 200
1.2.12.3.8. Wymagania dotyczące aktualizacji oprogramowania ... 200
1.2.12.3.9. Wymagania dotyczące testów odbiorowych ... 201
1.2.12.3.10. Wymagania dotyczące dokumentacji powykonawczej ... 201
1.2.12.3.11. Wymagania dotyczące gwarancji i wsparcia ... 202

1.2.12.3.12. Wymagania dotyczące bezpieczeństwa ... 202
1.2.12.3.13. Rezultat końcowy ... 203
1.2.13. Wymagania dla ośrodka zapasowego i łącza teleinformatycznego ... 203
1.2.13.1. Przedmiot wymagań ... 203
1.2.13.2. Cel utworzenia ośrodka zapasowego ... 204
1.2.13.3. Wymagania dotyczące zewnętrznego Data Center ... 204
1.2.13.4. Wymagania dotyczące lokalizacji zewnętrznego Data Center ... 206
1.2.13.5. Wymagania dotyczące szafy RACK i kolokacji zasobów Zamawiającego ... 207
1.2.13.6. Wymagania dotyczące zasilania i rozliczania energii elektrycznej ... 208
1.2.13.7. Wymagania dotyczące przyłącza światłowodowego 6J ... 208
1.2.13.8. Własność przyłącza światłowodowego ... 209
1.2.13.9. Wymagania dotyczące parametrów transmisyjnych i replikacji danych ... 210
1.2.13.10. Wymagania dotyczące bezpieczeństwa ... 210
1.2.13.11. Wymagania dotyczące utrzymania, kosztów i SLA ... 211
1.2.13.12. Wymagania dotyczące dokumentacji projektowej i formalnoprawnej ... 212
1.2.13.13. Wymagania dotyczące dokumentacji powykonawczej ... 213
1.2.13.14. Testy i odbiór ... 213
1.2.13.15. Gwarancja, utrzymanie i przekazanie do eksploatacji ... 214
1.2.13.16. Rezultat końcowy ... 215
1.2.14. Wymagania dla środowiska pracy zmodernizowanego systemu RIS ... 215
1.2.14.1. Przedmiot i cel wymagań ... 216
1.2.14.2. Docelowa architektura środowiska pracy ... 217
1.2.14.3. Analiza istniejących zasobów Zamawiającego ... 218
1.2.14.4. Warstwa obliczeniowa i wirtualizacyjna ... 219
1.2.14.4.1. Minimalne wymagania dla serwerów klastra środowiska pracy systemu RIS ... 220
1.2.14.5. Warstwa składowania danych ... 223
1.2.14.5.1. Minimalne wymagania dla macierzy dyskowych środowiska pracy systemu RIS ... 224
1.2.14.6. Warstwa LAN, SAN i urządzenia aktywne ... 228
1.2.14.7. Lokalizacja zapasowa i połączenie pomiędzy lokalizacjami ... 229
1.2.14.8. Backup, replikacja i odtwarzanie po awarii ... 230
1.2.14.9. Wysoka dostępność i odporność na awarie ... 231
1.2.14.10. Bezpieczeństwo środowiska ... 232
1.2.14.11. Monitoring techniczny i zarządzanie środowiskiem ... 233
1.2.14.12. Licencje, subskrypcje, wsparcie i aktualizacje ... 234
1.2.14.13. Kompletność dostawy i wdrożenia ... 235
1.2.14.14. Dokumentacja środowiska pracy ... 236
1.2.14.15. Testy i odbiór środowiska pracy ... 237
1.2.14.16. Szkolenie, przekazanie wiedzy i eksploatacja ... 239
1.2.14.17. Rezultat końcowy ... 240
1.2.15. Wymagania dla usług cyfrowych ... 240
1.2.15.1. Przedmiot i cel wymagań ... 240
1.2.15.2. Zakres usług cyfrowych objętych zamówieniem ... 240
1.2.15.3. Relacja do aplikacji mapowej i innych usług RIS ... 241
1.2.15.4. Wymagania ogólne dla systemu VTT ... 242
1.2.15.5. Obsługa map Inland ENC i warstw mapowych ... 242
1.2.15.6. Prezentacja aktualnego ruchu jednostek ... 243
1.2.15.7. Szczegółowe informacje o jednostkach ... 244
1.2.15.8. Wyszukiwanie jednostek i obiektów ... 245
1.2.15.9. Historia ruchu jednostek ... 246
1.2.15.10. Integracja z urządzeniami i podsystemami RIS ... 246
1.2.15.11. Wirtualne bramki, strefy, alarmy i powiadomienia ... 247
1.2.15.12. Narzędzia pomiarowe i funkcje ETA ... 248
1.2.15.13. Statystyki ruchu jednostek i raportowanie ... 248
1.2.15.14. Interfejs użytkownika ... 250
1.2.15.15. Administracja, role i uprawnienia ... 251
1.2.15.16. Dane, archiwizacja i jakość danych ... 251
1.2.15.17. Wydajność, skalowalność i niezawodność ... 252
1.2.15.18. Cyberbezpieczeństwo i ochrona dostępu ... 252
1.2.15.19. Monitoring techniczny usług cyfrowych ... 253
1.2.15.20. Dokumentacja ... 254

1.2.15.21. Szkolenia i przekazanie wiedzy ... 255
1.2.15.22. Testy i odbiór usług cyfrowych ... 256
1.2.15.23. Rezultat końcowy ... 257
1.2.16. Wymagania interoperacyjności, danych i integracji z systemami zewnętrznymi ... 257
1.2.16.1. Wymagania ogólne ... 258
1.2.16.2. Model danych, jakość danych i słowniki referencyjne ... 260
1.2.16.3. Usługa przekazywania danych do systemu EuRIS ... 261
1.2.16.4. Usługa przekazywania danych z wodowskazów systemu RIS do Systemu Hydrologii IMGW-PIB 265
1.2.16.4.1. Przedmiot i cel usługi ... 265
1.2.16.4.2. Zakres lokalizacyjny i czujniki objęte integracją ... 265
1.2.16.4.3. Wymagania dotyczące metody przekazywania danych ... 266
1.2.16.4.4. Wymagania dotyczące konfiguracji czujników i metadanych ... 267
1.2.16.4.5. Wymagania dotyczące harmonogramu i trybu pracy usługi ... 268
1.2.16.4.6. Wymagania dotyczące bezpieczeństwa i autoryzacji ... 268
1.2.16.4.7. Wymagania dotyczące walidacji i jakości danych ... 268
1.2.16.4.8. Wymagania dotyczące monitorowania, logowania i obsługi błędów ... 269
1.2.16.4.9. Wymagania dotyczące panelu administracyjnego ... 269
1.2.16.4.10. Wymagania dotyczące dokumentacji ... 270
1.2.16.4.11. Wymagania dotyczące testów i odbioru ... 271
1.2.16.4.12. Wymagania dotyczące skalowalności i utrzymania ... 272
1.2.16.5. API systemu RIS i udostępnianie danych dziedzinowych ... 272
1.2.16.6. Dokumentacja, bezpieczeństwo, testy i odbiór integracji ... 274
1.2.17. Dostępność cyfrowa ... 275
1.2.18. Cyberbezpieczeństwo, kontrola dostępu, monitoring i logowanie ... 280
1.2.18.1. Zakres odpowiedzialności Generalnego Wykonawcy ... 281
1.2.18.2. Segmentacja, strefy bezpieczeństwa i separacja ruchu ... 282
1.2.18.3. Bezpieczeństwo transmisji danych ... 283
1.2.18.4. Kontrola dostępu logicznego ... 283
1.2.18.5. Uwierzytelnianie i zarządzanie poświadczeniami ... 284
1.2.18.6. Zdalny dostęp administracyjny i serwisowy ... 285
1.2.18.7. Bezpieczeństwo aplikacji, usług cyfrowych i API ... 286
1.2.18.8. Bezpieczeństwo systemu CCTV ... 286
1.2.18.9. Bezpieczeństwo systemu VHF/AIS/DGNSS ... 287
1.2.18.10. Bezpieczeństwo czujników, sensorów i lokalnych komponentów akwizycji danych ... 288
1.2.18.11. Bezpieczeństwo szaf teletechnicznych i dostępu fizycznego ... 288
1.2.18.12. Monitoring techniczny i monitoring bezpieczeństwa ... 289
1.2.18.13. Logowanie zdarzeń i rozliczalność działań ... 290
1.2.18.14. Zarządzanie podatnościami, aktualizacjami i konfiguracją bezpieczeństwa ... 291
1.2.18.15. Kopie zapasowe konfiguracji i odtwarzanie ... 292
1.2.18.16. Ochrona danych i prywatności ... 293
1.2.18.17. Wymagania dotyczące testów bezpieczeństwa ... 293
1.2.18.18. Dokumentacja bezpieczeństwa ... 294
1.2.18.19. Wymagania eksploatacyjne i gwarancyjne ... 295
1.2.18.20. Wymagania odbiorowe ... 296
1.2.19. Wymagania dotyczące dokumentacji systemu RIS ... 297
1.2.19.1. Dokumentacja Administratora ... 298
1.2.19.2. Dokumentacja Użytkownika ... 298
1.2.19.3. Planu Ciągłości Działania BCP ... 300
1.2.19.4. Plan Odtworzenia po Awarii DRP ... 301
1.2.19.5. Polityka Zarządzania Podatnościami ... 302
1.2.19.5.1. Wymagania ogólne dotyczące dokumentu ... 302
1.2.19.5.2. Minimalna wymagana zawartość dokumentu ... 303
1.2.19.5.3. Wymagane załączniki do dokumentu ... 304
1.2.19.5.4. Wymagania eksploatacyjne po odbiorze ... 305
1.2.19.5.5. Wymagania odbiorowe i kryteria akceptacji dokumentu Polityka Zarządzania Podatnościami . 305
1.2.19.6. Dokumentacja eksploatacyjna systemu RIS ... 305
1.2.19.6.1. Obowiązek opracowania dokumentu ... 305
1.2.19.6.2. Cel dokumentu ... 306
1.2.19.6.3. Zakres zasobów objętych dokumentacją ... 307

1.2.19.6.4. Wymagania ogólne dotyczące dokumentu ... 308
1.2.19.6.5. Wykaz dokumentów powiązanych ... 309
1.2.19.6.6. Struktura opisu podsystemów i komponentów ... 309
1.2.19.6.7. Procedury operacyjne ... 310
1.2.19.6.8. Metody zapewnienia wymaganego poziomu niezawodności ... 311
1.2.19.6.9. Procedury okresowych testów ... 312
1.2.19.6.10. Procedury konserwacji ... 312
1.2.19.6.11. Procedury awaryjne i diagnostyczne ... 313
1.2.19.6.12. Kopie zapasowe i odtwarzanie ... 314
1.2.19.6.13. Aktualizacje oprogramowania i konfiguracji ... 314
1.2.19.6.14. Zróżnicowanie zawartości ze względu na charakter podsystemów i komponentów ... 315
1.2.19.6.14.1. Dla oprogramowania aplikacyjnego i usług cyfrowych: ... 315
1.2.19.6.14.2. Dla infrastruktury serwerowej, wirtualizacyjnej i pamięci masowej: ... 315
1.2.19.6.14.3. Dla infrastruktury sieciowej, transmisyjnej i cyberbezpieczeństwa: ... 316
1.2.19.6.14.4. Dla urządzeń terenowych, sensorów i komponentów pomiarowych: ... 316
1.2.19.6.14.5. Dla systemów radiokomunikacyjnych i antenowych: ... 316
1.2.19.6.14.6. Dla systemów CCTV i rejestracji obrazu: ... 316
1.2.19.6.14.7. Dla systemów zasilania, klimatyzacji, kontroli dostępu, ochrony przeciwpożarowej i infrastruktury technicznej obiektów: ... 316
1.2.19.6.14.8. Dla interfejsów integracyjnych i wymiany danych: ... 316
1.2.19.6.14.9. Wykazy i zestawienia wymagane w dokumentacji ... 317
1.2.19.6.15. Wymagania dotyczące aktualizacji dokumentu ... 319
1.2.19.6.16. Wymagania dotyczące formy przekazania ... 319
1.2.19.6.17. Warunki akceptacji dokumentu ... 319
1.2.20. Procedury odbioru i testowania całości systemu RIS ... 320
1.2.21. Szkolenia, procedury operacyjne i przekazanie do eksploatacji ... 324
1.2.22. Gwarancja, serwis, obsługa techniczna i SLA ... 328
1.2.23. Przeglądy techniczne i aktualizacje oprogramowania w okresie gwarancji ... 334
1.2.23.1. Założenie ogólne ... 334
1.2.23.2. Obowiązek opracowania dokumentu ... 335
1.2.23.3. Charakter dokumentu ... 335
1.2.23.4. Minimalny zakres środowiska objętego analizą ... 336
1.2.23.5. Wyłączenie zasobów historycznych ... 337
1.2.23.6. Wymagana zawartość dokumentu ... 337
1.2.23.7. Minimalna częstotliwość czynności ... 338
1.2.23.8. Zakres czynności serwisowych i obsługi technicznej ... 338
1.2.23.9. Aktualizacje oprogramowania ... 339
1.2.23.10. Raportowanie ... 340
1.2.23.11. Aktualizacja dokumentu ... 341
1.2.23.12. Minimalne tabele wymagane w dokumencie ... 341
1.2.23.13. Warunki akceptacji dokumentu ... 343
1.2.24. Usługa Utrzymania ... 343
1.2.25. Ogólne wymagania dotyczące przedmiotu dostaw realizowanych przez Generalnego Wykonawcę ... 345

2. CZĘŚĆ INFORMACYJNA ... 349

2.1. PRZEPISY PRAWNE, NORMY I STANDARDY ZWIĄZANE Z PROJEKTOWANIEM I WYKONANIEM ZAMIERZENIA INWESTYCYJNEGO ... 349
2.1.1. Przepisy prawne Unii Europejskiej ... 349
2.1.1.1. Usługi informacji rzecznej RIS, żegluga śródlądowa i sieć TEN-T ... 349
2.1.1.2. Usługi cyfrowe, dane, cyberbezpieczeństwo, interoperacyjność i dostępność ... 350
2.1.1.3. Wyroby, urządzenia, kompatybilność elektromagnetyczna i wymagania produktowe ... 352
2.1.1.4. Środowisko, gospodarka wodna, oceny oddziaływania i finansowanie UE ... 353
2.1.2. Umowy międzynarodowe ... 354
2.1.3. Polskie przepisy prawne w randze ustawy ... 354
2.1.3.1. Zamówienia publiczne, umowy, finanse publiczne i realizacja inwestycji ... 354
2.1.3.2. Żegluga śródlądowa, RIS, gospodarka wodna i drogi wodne ... 355
2.1.3.3. Budownictwo, planowanie przestrzenne, geodezja, drogi i przeszkody lotnicze ... 355
2.1.3.4. Komunikacja elektroniczna, radiokomunikacja, cyberbezpieczeństwo, dane i dostępność cyfrowa . 356

2.1.3.5. Środowisko, odpady, BHP i ochrona przeciwpożarowa ... 358
2.1.4. Polskie przepisy prawne w randze rozporządzenia ... 358
2.1.4.1. PFU, dokumentacja projektowa, projekt budowlany i warunki techniczne obiektów ... 358
2.1.4.2. RIS, żegluga śródlądowa i drogi wodne ... 359
2.1.4.3. Radiokomunikacja, częstotliwości, urządzenia radiowe i pola elektromagnetyczne ... 360
2.1.4.4. Ochrona środowiska, odpady, oceny oddziaływania i gospodarka wodna ... 360
2.1.4.5. BHP, ochrona przeciwpożarowa, organizacja robót i utrzymanie ruchu ... 361
2.1.4.6. Krajowe Ramy Interoperacyjności i systemy teleinformatyczne administracji publicznej ... 362
2.1.4.7. Przepisy prawa miejscowego i akty właściwych organów dla Odrzańskiej Drogi Wodnej ... 362
2.1.5. Normy i standardy techniczne ... 363
2.1.5.1. RIS, Inland ECDIS, Inland AIS, ERI, NtS i dane referencyjne ... 363
2.1.5.2. Radiokomunikacja VHF, AIS, DGNSS, propagacja i urządzenia radiowe ... 363
2.1.5.3. CCTV/VSS, transmisja i zapis obrazu ... 364
2.1.5.4. Sieci IP, transmisja danych, synchronizacja czasu i zarządzanie ... 365
2.1.5.5. Cyberbezpieczeństwo, bezpieczeństwo informacji i ciągłość działania ... 365
2.1.5.6. Okablowanie, serwerownie, zasilanie, EMC i urządzenia elektryczne ... 366
2.1.5.7. Konstrukcje budowlane, wieże, maszty, wsporniki, fundamenty i zabezpieczenia antykorozyjne ... 367
2.1.5.8. Jakość, zarządzanie projektem, testy, niezawodność i utrzymanie ... 367
2.1.5.9. Dostępność cyfrowa, WCAG i dostępność produktów oraz usług ICT ... 368
2.1.6. Pozostałe dokumenty programowe, wytyczne i dokumenty odniesienia ... 369
2.1.6.1. Dokumenty programowe i finansowanie ... 369
2.1.6.2. Dokumenty strategiczne i branżowe dla żeglugi śródlądowej, transportu i gospodarki wodnej ... 369
2.1.6.3. Dokumenty odniesienia dla systemu RIS i komponentów teleinformatycznych ... 370
2.2. INFORMACJE I DOKUMENTY NIEZBĘDNE DO ZAPROJEKTOWANIA ROBÓT BUDOWLANYCH ORAZ WYKONANIA ZAMIERZENIA INWESTYCYJNEGO ... 370
2.2.1. Postanowienia ogólne ... 370
2.2.2. Zakres dokumentacji projektowej wymaganej w ramach Zamówienia ... 371
2.2.3. Mapy, materiały geodezyjne i obsługa geodezyjna ... 372
2.2.4. Operat Techniczny z pomiarów wodowskazów ... 373
2.2.5. Badania gruntowo-wodne i geotechniczne warunki posadowienia ... 374
2.2.6. Dokumentacja dla nowych wież antenowych VHF/AIS ... 375
2.2.7. Dokumentacja rozbiórki istniejących wież, masztów i konstrukcji ... 376
2.2.8. Dokumentacja wodnoprawna i wymagania wynikające z Prawa wodnego ... 376
2.2.9. Wymagania PGW Wody Polskie dla lokalizacji wież antenowych VHF/AIS ... 377
2.2.10. Montaż kamer, wodowskazów i czujników na istniejących obiektach hydrotechnicznych ... 379
2.2.11. Montaż infrastruktury RIS na obiektach mostowych, drogowych i kolejowych ... 380
2.2.12. Projekty przyłączy elektroenergetycznych, zasilania i tras kablowych ... 380
2.2.13. Uzgodnienia konserwatorskie i archeologiczne ... 381
2.2.14. Inwentaryzacja zieleni i ochrona przyrody ... 381
2.2.15. Raporty, opinie i ekspertyzy z zakresu ochrony środowiska ... 382
2.2.16. Inwentaryzacja i ekspertyzy istniejących obiektów budowlanych ... 382
2.2.17. Porozumienia, zgody, pozwolenia oraz warunki techniczne i realizacyjne ... 383
2.2.18. Pozwolenia radiowe, analizy radiowe i oddziaływanie pól elektromagnetycznych ... 384
2.2.19. Oznakowanie przeszkodowe i uwarunkowania lotnicze ... 384
2.2.20. Dokumentacja dla robót w czynnym systemie RIS i na czynnych obiektach ... 385
2.2.21. Lokalizacje zamienne ... 385
2.2.22. Dokumentacja odbiorowa, powykonawcza i eksploatacyjna ... 386
2.2.23. Dodatkowe wytyczne inwestorskie i uwarunkowania związane z finansowaniem ... 387

3. SPIS TABEL ... 389

4. SPIS RYSUNKÓW ... 390

5. ZAŁĄCZNIKI ... 391

ZAŁĄCZNIK NR 1 - SCHEMAT ROZKŁADU POMIESZCZEŃ OBJĘTYCH MODERNIZACJĄ SIECI TELEINFORMATYCZNEJ ... 392
ZAŁĄCZNIK NR 2 – WYKAZ STOSOWANYCH SKRÓTÓW I POJĘĆ ... 394

Streszczenie

Program Funkcjonalno-Użytkowy dla projektu „Rozbudowa systemu RIS na Odrzańskiej Drodze Wodnej” określa zakres, założenia oraz wymagania Zamawiającego dla realizacji kolejnego etapu rozwoju systemu usług informacji rzecznej RIS. Projekt jest realizowany na rzecz Urzędu Żeglugi Śródlądowej w Szczecinie i ma na celu rozszerzenie terytorialnego zasięgu działania systemu RIS na kolejne odcinki Odrzańskiej Drogi Wodnej, a także zwiększenie dostępności, kompletności i jakości informacji wykorzystywanych do nadzoru nad żeglugą śródlądową.

Zasadniczą logiką przedsięwzięcia jest rozszerzenie terytorialnego zasięgu działania systemu RIS na Odrzańskiej Drodze Wodnej. Podstawowy obszar rozbudowy obejmuje odcinek ODW od Ścinawy do Koźla wraz z powiązanymi odgałęzieniami dróg wodnych, w tym obszar Wrocławskiego Węzła Wodnego, który ze względu na koncentrację dróg wodnych, obiektów hydrotechnicznych, mostów i infrastruktury miejskiej ma szczególne znaczenie operacyjne dla żeglugi oraz administracji drogi wodnej. Uzupełniająco projekt obejmuje również punktowe lokalizacje oraz zadania modernizacyjne realizowane na obszarze aktualnie działającego systemu RIS Dolnej Odry, w zakresie niezbędnym do zapewnienia spójności technicznej, funkcjonalnej, transmisyjnej i eksploatacyjnej całego systemu RIS. Rozszerzenie zasięgu terytorialnego systemu wymaga wykonania nowej infrastruktury terenowej, rozbudowy sieci transmisji danych, dostosowania zaplecza technicznego Centrum RIS, wdrożenia dodatkowych usług cyfrowych oraz zapewnienia integracji nowych elementów z istniejącym systemem RIS.

Przedmiot zamówienia będzie realizowany w formule „zaprojektuj i zbuduj”. Generalny Wykonawca będzie odpowiedzialny za przygotowanie dokumentacji projektowej, uzyskanie wymaganych uzgodnień i pozwoleń, wykonanie robót, dostaw, instalacji, konfiguracji, integracji, testów oraz przekazanie do eksploatacji kompletnego i zintegrowanego systemu. Program Funkcjonalno-Użytkowy stanowi podstawę do przygotowania dokumentacji postępowania o udzielenie zamówienia publicznego oraz określa minimalne wymagania Zamawiającego wobec rozwiązań projektowanych i wykonywanych przez Generalnego Wykonawcę.

Rozszerzenie zasięgu działania systemu RIS obejmuje w szczególności rozbudowę infrastruktury radiokomunikacyjnej VHF/AIS/DGNSS. W ramach tego obszaru przewidziano budowę nowych stacji i elementów infrastruktury radiowej umożliwiających objęcie usługami łączności i identyfikacji jednostek kolejnych odcinków drogi wodnej. Rozbudowana infrastruktura VHF/AIS/DGNSS ma zapewnić poprawę pokrycia radiowego, odbiór danych Inland AIS, obsługę komunikacji głosowej VHF, dystrybucję poprawek DGNSS oraz integrację nowych lokalizacji z Centrum RIS.

Istotnym elementem projektu jest również rozbudowa i modernizacja systemu monitoringu wizyjnego CCTV. Nowe i modernizowane punkty kamerowe mają wspierać obserwację drogi wodnej, mostów, śluz, nabrzeży, obiektów hydrotechnicznych oraz innych miejsc istotnych z punktu widzenia bezpieczeństwa żeglugi. Rozbudowa CCTV jest bezpośrednio powiązana z rozszerzeniem terytorialnym systemu RIS, ponieważ umożliwia operatorom Centrum RIS uzyskanie obrazu z nowych lokalizacji objętych projektem oraz uzupełnia dane pozyskiwane z systemów radiowych i pomiarowych.

W celu zapewnienia informacji o warunkach na drodze wodnej projekt obejmuje instalację nowych czujników hydrologicznych oraz sensorów meteorologicznych. Czujniki hydrologiczne mają umożliwiać bieżący pomiar poziomu wody w wybranych lokalizacjach, natomiast sensory

meteorologiczne mają dostarczać dane o podstawowych warunkach atmosferycznych, w tym o wietrze, temperaturze, wilgotności, ciśnieniu i opadach. Rozbudowa tych komponentów pozwoli rozszerzyć zakres informacji hydrometeorologicznej dostępnej w systemie RIS na nowe odcinki Odrzańskiej Drogi Wodnej.

Rozszerzenie zasięgu terytorialnego systemu wymaga również rozbudowy sieci transmisji danych. Sieć ta ma zapewnić bezpieczne i niezawodne połączenie nowych lokalizacji terenowych z Centrum RIS oraz umożliwić przesył danych z kamer, stacji AIS, urządzeń VHF, czujników hydrologicznych, sensorów meteorologicznych, systemów zasilania, monitoringu technicznego i innych komponentów infrastruktury. Wymagania PFU obejmują zapewnienie odpowiedniej przepustowości, redundancji, bezpieczeństwa transmisji, monitorowania, zarządzania oraz możliwości dalszej rozbudowy sieci.

Projekt przewiduje także wykonanie infrastruktury terenowej niezbędnej do instalacji urządzeń RIS w nowych lokalizacjach. Obejmuje to w szczególności wieże, maszty, konstrukcje wsporcze, słupy kamerowe, szafy teletechniczne, systemy zasilania, instalacje odgromowe, uziemienia, zabezpieczenia przepięciowe, ogrodzenia, dostęp serwisowy i inne elementy towarzyszące. Infrastruktura ta stanowi techniczną podstawę rozszerzenia systemu RIS na nowe obszary i musi zostać zaprojektowana z uwzględnieniem warunków terenowych, formalnoprawnych, środowiskowych, hydrotechnicznych, eksploatacyjnych i utrzymaniowych.

Równolegle z rozbudową infrastruktury terenowej PFU obejmuje modernizację i doposażenie zaplecza technicznego Zamawiającego. Zakres ten obejmuje m.in. doposażenie serwerowni głównej, modernizację serwerowni pełniącej rolę węzła telekomunikacyjnego, modernizację sieci teleinformatycznej w siedzibie Zamawiającego, utworzenie środowiska pracy zmodernizowanego systemu RIS oraz utworzenie serwerowni zapasowej wraz z łączem teleinformatycznym do Centrum RIS. Celem tych działań jest zapewnienie, aby centralna infrastruktura systemu była przygotowana do obsługi większej liczby lokalizacji, większego wolumenu danych, nowych usług cyfrowych oraz wymagań dotyczących wysokiej dostępności, backupu, replikacji i odtwarzania po awarii.

W ramach projektu przewidziano wdrożenie usług cyfrowych RIS, w tym systemu VTT służącego do śledzenia i namierzania jednostek. System VTT ma umożliwiać operatorom Centrum RIS prezentację aktualnego ruchu jednostek na mapie, obsługę danych Inland AIS, dostęp do historii ruchu, wyszukiwanie jednostek, tworzenie wirtualnych bramek i stref, generowanie alarmów, obliczanie ETA oraz przygotowywanie statystyk i raportów ruchu. Usługi cyfrowe mają wykorzystywać dane z nowych i istniejących elementów infrastruktury RIS, wspierając w ten sposób praktyczne wykorzystanie rozszerzonego terytorialnie systemu.

PFU określa także wymagania interoperacyjności, danych i integracji z systemami zewnętrznymi. Szczególne znaczenie mają wymagania dotyczące przekazywania danych do EuRIS, udostępniania danych poprzez API systemu RIS oraz przekazywania danych z wodowskazów systemu RIS do Systemu Hydrologii IMGW-PIB. Integracje te mają umożliwić wykorzystanie danych pozyskiwanych z rozszerzonego obszaru działania systemu RIS nie tylko przez Centrum RIS, ale również przez inne systemy, instytucje i uprawnionych interesariuszy.

Dokument określa również wymagania przekrojowe dotyczące zgodności prawnej i normatywnej, cyberbezpieczeństwa, dostępności cyfrowej, dokumentacji, testowania, odbiorów, szkoleń, gwarancji, przeglądów technicznych i utrzymania. Wymagania te mają zapewnić, że

rozbudowany system RIS będzie rozwiązaniem kompletnym, bezpiecznym, interoperacyjnym, możliwym do eksploatacji i dalszego rozwoju. Szczegółowe procedury realizacyjne, testowe, odbiorowe i utrzymaniowe mają potwierdzić prawidłowe wykonanie przedmiotu zamówienia oraz przygotowanie systemu do stabilnej pracy po zakończeniu projektu.

Realizacja projektu ma doprowadzić do powstania spójnego, zintegrowanego i skalowalnego systemu RIS obejmującego rozszerzony obszar Odrzańskiej Drogi Wodnej. Rozbudowany system ma zapewnić lepsze pokrycie usługami informacji rzecznej, większą dostępność danych o ruchu jednostek i warunkach nawigacyjnych, sprawniejsze monitorowanie sytuacji na drodze wodnej, skuteczniejszą wymianę danych z systemami zewnętrznymi oraz wyższy poziom bezpieczeństwa i efektywności żeglugi śródlądowej.

Abstract

The Functional and Utility Programme for the project “Extension of the RIS System on the Oder Waterway” defines the scope, assumptions and requirements of the Contracting Authority for the next stage of development of River Information Services in Poland. The project is carried out for the Inland Navigation Office in Szczecin and aims to extend the territorial coverage of the existing RIS system on the Oder Waterway, improve the availability and quality of navigation-related information, and enhance the safety and efficiency of inland waterway transport.

The main objective of the project is to expand the RIS system to additional sections of the Oder Waterway. The primary extension area covers the section from Ścinawa to Koźle, including related branches of inland waterways and the Wrocław Waterway Junction, which is of particular operational importance due to the concentration of waterways, hydraulic structures, bridges and urban infrastructure. In addition, the project includes selected point locations and modernisation tasks within the area of the already operational RIS system on the Lower Oder, to ensure technical, functional, transmission and operational consistency of the entire RIS environment.

The contract will be implemented under the “design and build” formula. The General Contractor will be responsible for preparing the design documentation, obtaining the required arrangements, permits and approvals, carrying out works and deliveries, installing and configuring equipment and systems, integrating new and existing components, conducting tests and commissioning activities, and handing over a complete, integrated and operational RIS system. The Functional and Utility Programme constitutes the baseline document for preparing the public procurement documentation and defines the minimum requirements to be met by the solutions designed and implemented by the General Contractor.

The territorial extension of the RIS system includes, in particular, the development of VHF/AIS/DGNSS radio communication infrastructure. The project provides for new radio stations and related infrastructure enabling further sections of the waterway to be covered by communication and vessel identification services. The extended VHF/AIS/DGNSS infrastructure is intended to improve radio coverage, support Inland AIS data reception, enable VHF voice communication, provide DGNSS correction services, and integrate new field locations with the RIS Centre.

A further important component of the project is the extension and modernisation of the CCTV video surveillance system. New and upgraded camera points will support the observation of

waterways, bridges, locks, quays, hydraulic structures and other locations relevant to navigation safety. The CCTV extension is directly linked to the territorial expansion of the RIS system, as it will provide RIS Centre operators with visual information from the new locations covered by the project and complement data obtained from radio, hydrological and meteorological systems.

To improve the availability of information on waterway conditions, the project includes the installation of new hydrological gauges and meteorological sensors. Hydrological sensors will enable continuous water level measurement at selected locations, while meteorological sensors will provide data on key atmospheric parameters, including wind, temperature, humidity, pressure and precipitation. These components will extend the scope and territorial coverage of hydro-meteorological information available within the RIS system.

The extended RIS coverage also requires the development of the data transmission network. This network must ensure secure and reliable communication between the new field locations and the RIS Centre and enable the transmission of data from cameras, AIS stations, VHF devices, hydrological gauges, meteorological sensors, power supply systems, technical monitoring systems and other RIS infrastructure components. The Functional and Utility Programme defines requirements for bandwidth, redundancy, transmission security, monitoring, management and future scalability of the network.

The project also includes the field infrastructure necessary for installing RIS equipment in new locations. This includes towers, masts, supporting structures, camera poles, outdoor telecommunication cabinets, power supply systems, lightning protection, earthing, surge protection, fencing, service access and other auxiliary elements. This infrastructure forms the technical foundation for extending the RIS system to new areas and must be designed with regard to local site conditions, legal and administrative requirements, environmental constraints, hydraulic structures, operational needs and maintenance requirements.

In parallel with the development of field infrastructure, the project provides for the modernisation and enhancement of the Contracting Authority’s technical facilities. This includes additional equipment for the main server room, modernisation of the server room acting as a telecommunication node, modernisation of the local telecommunication network at the Contracting Authority’s premises, establishment of the operating environment for the upgraded RIS system, and creation of a backup server room together with a telecommunication link to the RIS Centre. These measures are intended to ensure that the central infrastructure is capable of supporting a larger number of field locations, increased data volumes, new digital services and requirements related to high availability, backup, replication and disaster recovery.

The project also provides for the implementation of RIS digital services, including a Vessel Tracking and Tracing system. The VTT system will enable RIS Centre operators to display current vessel traffic on a map, process Inland AIS data, access vessel movement history, search for vessels, define virtual gates and zones, generate alarms, calculate ETA, and prepare traffic statistics and reports. Digital services will use data from both existing and new RIS infrastructure elements and will support the operational use of the territorially extended RIS system.

The Functional and Utility Programme also defines requirements for interoperability, data management and integration with external systems. Particular importance is assigned to data exchange with EuRIS, the provision of RIS domain data through APIs, and the transfer of water level data from RIS gauges to the Hydrology System of the Institute of Meteorology and Water

Management – National Research Institute. These integrations are intended to enable data collected from the extended RIS area to be used not only by the RIS Centre, but also by other systems, institutions and authorised stakeholders.

The document also sets out cross-cutting requirements concerning legal and regulatory compliance, cybersecurity, digital accessibility, documentation, testing, acceptance, training, warranty, technical inspections and maintenance. These requirements are intended to ensure that the extended RIS system is complete, secure, interoperable, maintainable and ready for further development. The implementation, testing, commissioning and maintenance procedures will confirm the proper execution of the contract and the readiness of the system for stable operation after project completion.

The implementation of the project will result in a coherent, integrated and scalable RIS system covering an extended area of the Oder Waterway. The upgraded system is expected to provide broader RIS service coverage, improved availability of data on vessel traffic and navigation conditions, more effective monitoring of the waterway situation, enhanced data exchange with external systems, and a higher level of safety and efficiency of inland navigation.

1. Część opisowa

1.1. Opis ogólny przedmiotu zamówienia

Przedmiotem zamówienia jest zaprojektowanie i wykonanie rozbudowy systemu RIS na Odrzańskiej Drodze Wodnej w ramach projektu pn. „Rozbudowa systemu RIS na Odrzańskiej Drodze Wodnej”. Zamówienie obejmuje przygotowanie dokumentacji projektowej, wykonanie niezbędnych uzgodnień i czynności formalnoprawnych, dostawę, montaż, konfigurację, integrację, testowanie oraz uruchomienie infrastruktury technicznej, teleinformatycznej i aplikacyjnej niezbędnej do świadczenia usług informacji rzecznej RIS na rozszerzonym obszarze systemu.

Projekt będzie realizowany w formule „zaprojektuj i zbuduj”. Oznacza to, że Wykonawca jest odpowiedzialny za kompleksowe doprecyzowanie rozwiązań projektowych na podstawie niniejszego Programu Funkcjonalno-Użytkowego, załączników, Studium Wykonalności, konsultacji z Zamawiającym oraz wyników własnych analiz technicznych i lokalizacyjnych. Wykonawca zobowiązany będzie do zapewnienia kompletności, spójności i interoperacyjności wdrażanego rozwiązania, a także do takiego zaprojektowania systemu, aby jego poszczególne elementy tworzyły jednolite środowisko techniczne i usługowe systemu RIS.

Zakres zamówienia obejmuje w szczególności rozbudowę infrastruktury radiokomunikacyjnej VHF/AIS, infrastruktury obserwacyjnej i czujnikowej, sieci transmisji danych, infrastruktury serwerowej oraz warstwy usług cyfrowych RIS. Przedmiot zamówienia obejmuje również modernizację wybranych elementów istniejącego systemu RIS oraz integrację nowych komponentów z funkcjonującą infrastrukturą, narzędziami operatorskimi i usługami udostępnianymi użytkownikom śródlądowych dróg wodnych.

Celem zamówienia jest uzyskanie zintegrowanego, skalowalnego i gotowego do dalszego rozwoju terytorialnego i funkcjonalnego systemu RIS, który będzie wspierał bezpieczeństwo i efektywność żeglugi śródlądowej, zapewniał dostęp do aktualnych informacji o warunkach na drodze wodnej oraz umożliwiał wykorzystanie danych pochodzących z urządzeń terenowych, jednostek pływających i zewnętrznych źródeł danych. System ma zapewniać obsługę usług RIS zgodnie z obowiązującymi wymaganiami prawnymi, standardami europejskimi oraz wymaganiami interoperacyjności, w tym w zakresie współpracy z rozwiązaniami krajowymi i europejskimi.

Niniejszy rozdział przedstawia ogólne ujęcie przedmiotu zamówienia. Szczegółowe założenia projektu, w tym cel i logika interwencji, analiza stanu istniejącego, zakres terytorialny, zakres rzeczowy inwestycji, zasady weryfikacji lokalizacji, wymagania interoperacyjności oraz powiązania z systemami i usługami RIS, zostały opisane w kolejnych podrozdziałach niniejszego rozdziału oraz w dalszych częściach PFU. Szczegółowe wymagania techniczne dla wybranych obszarów wdrożenia zostały zamieszczone w załącznikach:

1) Plan systemu monitoringu wizyjnego,
2) Plan łączności radiowej VHF/AIS,
3) Plan połączeń transmisyjnych.

1.1.1. Generalne założenia projektu rozbudowy RIS na ODW

Projekt pn. „Rozbudowa systemu RIS na Odrzańskiej Drodze Wodnej” stanowi kolejny etap rozwoju zharmonizowanych usług informacji rzecznej RIS w Polsce. Przedsięwzięcie jest kontynuacją wcześniejszych działań realizowanych przez Urząd Żeglugi Śródlądowej w Szczecinie, w szczególności projektu „Pełne wdrożenie RIS Dolnej Odry”. Celem rozbudowy jest zwiększenie obszaru objętego systemem RIS, poprawa funkcjonalności systemu już eksploatowanego oraz zapewnienie spójnego środowiska informacyjnego dla użytkowników śródlądowych dróg wodnych.

Rozbudowa systemu RIS na ODW obejmuje zarówno rozwój infrastruktury terenowej, jak i modernizację warstwy centralnej, aplikacyjnej oraz usługowej. Projekt zakłada realizację nowych obiektów stacji radiokomunikacyjnych VHF/AIS, budowę i uruchomienie obiektów stacji czujnikowych obejmujących kamery oraz czujniki hydrologiczne i meteorologiczne, wymianę wybranych obecnie eksploatowanych urządzeń i elementów systemu RIS, dostawę i montaż infrastruktury serwerowej wraz z modernizacją pomieszczenia serwerowni oraz realizację usług cyfrowych systemu RIS.

System ma zostać zaprojektowany jako zintegrowane rozwiązanie obejmujące cztery zasadnicze warstwy funkcjonalne:

1) segment źródeł danych (sensorów),
2) segment transmisji danych,
3) segment operatorów,
4) segment użytkowników.

Segment źródeł danych obejmuje w szczególności stacje brzegowe AIS/DGNSS, stacje brzegowe VHF, kamery obserwacyjne i dozorowe CCTV, wodowskazy, czujniki meteorologiczne oraz inne elementy pomiarowe i obserwacyjne.

Segment transmisji danych odpowiada za bezpieczne i stabilne przekazywanie danych z obiektów terenowych (lokalizacji instalacji infrastruktury RIS) do Centrum RIS i w kierunku odwrotnym dla zadań propagacji danych oraz zadań administrowania i zarządzania systemem.

Segment operatorów obejmuje narzędzia i stanowiska umożliwiające świadczenie usług RIS, natomiast segment użytkowników obejmuje administrację publiczną, armatorów, kierowników statków, profesjonalnych i nieprofesjonalnych użytkowników śródlądowych dróg wodnych oraz inne uprawnione instytucje korzystających z usług cyfrowych udostępnianych przez Centrum RIS.

Przedmiot zamówienia jest realizowany w formule „zaprojektuj i zbuduj”. Oznacza to, że szczegółowe rozwiązania techniczne, lokalizacyjne, konstrukcyjne, transmisyjne i aplikacyjne zostaną zweryfikowane i doprecyzowane na etapie projektowania przez Generalnego Wykonawcę.

Generalny Wykonawca będzie zobowiązany do zapewnienia kompletności rozwiązania, w tym do weryfikacji wykonalności lokalizacji wskazanych w Programie Funkcjonalno-Użytkowym oraz

towarzyszących mu załącznikach, przygotowania dokumentacji projektowej zgodnej z obowiązującymi przepisami prawa oraz standardami branżowymi, pozyskania wymaganych uzgodnień oraz pozwoleń, wykonania robót, dostawy komponentów systemu RIS, integracji wewnętrznej komponentów systemu w celu uzyskania systemu w pełni zintegrowanego, integracji systemu RIS z systemami zewnętrznymi, uruchomienia, testowania oraz przekazania rozwiązania do eksploatacji.

1.1.1.1. Cel, tło i logika interwencji

Podstawowym celem projektu jest opracowanie i świadczenie nowych oraz zmodernizowanych usług RIS dla administracji publicznej, armatorów żeglugi śródlądowej, kierowników statków oraz pozostałych zainteresowanych podmiotów. Projekt ma umożliwić zintegrowanie i wykorzystanie informacji pochodzących ze wszystkich czujników systemu RIS, urządzeń AIS instalowanych na jednostkach pływających oraz zewnętrznych źródeł danych. W efekcie system powinien wspierać bezpieczeństwo żeglugi, poprawiać dostępność informacji o drodze wodnej, zwiększać przewidywalność warunków nawigacyjnych oraz wzmacniać możliwość zarządzania ruchem i reagowania na zdarzenia.

Logika interwencji opiera się na założeniu, że rozwój żeglugi śródlądowej na Odrzańskiej Drodze Wodnej wymaga nie tylko modernizacji infrastruktury hydrotechnicznej i utrzymaniowej, ale również zapewnienia użytkownikom drogi wodnej wiarygodnych, aktualnych i łatwo dostępnych informacji. RIS jest narzędziem, które pozwala przetwarzać dane o ruchu statków, warunkach hydrologicznych, meteorologicznych, sytuacji na torze wodnym, prześwitach pod mostami, obrazie z kamer oraz komunikatach żeglugowych w spójne usługi informacyjne. Dzięki temu kierownicy statków i operatorzy systemu mogą podejmować decyzje w oparciu o aktualny obraz sytuacji na drodze wodnej.

Projekt odpowiada na potrzebę rozszerzenia obszaru funkcjonowania systemu informacji rzecznej poza dotychczasowy zakres systemu RIS. Istniejący system obejmuje przede wszystkim odcinek Odry od mostu autostradowego A2 w Świecku do granicy z morskimi wodami wewnętrznymi oraz odcinek Warty od ujścia do Odry do Nadzoru Wodnego w Świerkocinie. Rozbudowa ma objąć kolejny istotny fragment Odrzańskiej Drogi Wodnej, w tym obszar Wrocławskiego Węzła Wodnego, który ze względu na zagęszczenie infrastruktury hydrotechnicznej i znaczenie dla żeglugi wymaga szczególnego wsparcia informacyjnego.

Interwencja ma również wymiar systemowy. Projekt ma doprowadzić do tego, aby system RIS był rozwijany jako jednolity, skalowalny i możliwy do dalszej rozbudowy system krajowy, kompatybilny z rozwiązaniami europejskimi. W tym znaczeniu PFU opisuje nie tylko dostawę pojedynczych urządzeń i aplikacji, lecz także docelowy sposób współdziałania podsystemów, danych, usług, operatorów i użytkowników.

1.1.1.2. Analiza stanu istniejącego i doświadczeń z wcześniejszych wdrożeń

Stan istniejący systemu RIS w Polsce jest wynikiem kilku kolejnych etapów wdrożeniowych. Po zakończeniu projektu „Pełne wdrożenie RIS Dolnej Odry” infrastruktura terenowa systemu RIS obejmuje 40 lokalizacji, w których rozmieszczono różnego rodzaju sensory, w tym wodowskazy,

stacje meteorologiczne, kamery stacjonarne i PTZ, urządzenia przewodowej i radiowej transmisji danych, urządzenia łączności radiowej VHF oraz urządzenia AIS/DGPS. Obiekty te tworzą funkcjonalny system pozyskiwania danych, ich transmisji do Centrum RIS oraz udostępniania informacji operatorom i użytkownikom.

Dotychczasowe wdrożenia potwierdziły zasadność stosowania podstawowych technologii RIS, w szczególności AIS, DGPS, VHF, elektronicznych map nawigacyjnych, komunikatów dla kierowników statków, monitoringu hydrometeorologicznego oraz monitoringu wizyjnego. Jednocześnie doświadczenia eksploatacyjne wskazują, że system powinien być rozwijany z większym naciskiem na integrację usług, ergonomię narzędzi operatorskich, dostępność danych dla użytkowników zewnętrznych, automatyzację informacji o stanie infrastruktury oraz poprawę niezawodności transmisji danych.

W obszarze monitoringu wizyjnego istotne znaczenie ma możliwość obserwacji sytuacji na drodze wodnej, w tym ruchu jednostek, warunków lodowych, zdarzeń nietypowych i sytuacji wymagających późniejszej analizy. Monitoring z wykorzystaniem kamer przemysłowych może być wykorzystywany przy rozpatrywaniu zdarzeń, skarg i spraw wypadkowych, a także przy wspieraniu działań administracji drogi wodnej. Dotychczasowe doświadczenia wskazują, że obserwacja wizyjna jest jednym z najbardziej intuicyjnych źródeł informacji dla operatora RIS, ale wymaga stabilnej transmisji, właściwej jakości obrazu, archiwizacji i łatwego udostępniania uprawnionym użytkownikom.

W obszarze transmisji danych kluczowe znaczenie ma zapewnienie stabilnego połączenia pomiędzy obiektami terenowymi a Centrum RIS. System musi zapewniać transmisję danych z kamer, stacji AIS, stacji VHF, wodowskazów, stacji meteorologicznych i urządzeń diagnostycznych. Ze względu na znaczną rozległość obszaru oraz zróżnicowane warunki lokalizacyjne należy przewidzieć rozwiązania podstawowe i zapasowe, a dla lokalizacji o znaczeniu krytycznym mechanizmy redundancji oraz monitorowania jakości połączeń.

W obszarze usług cyfrowych istniejący system obejmuje m.in. usługę VTT, usługi hydrometeorologiczne, stronę internetową RIS oraz narzędzia do udostępniania danych użytkownikom. Analiza stanu bieżącego wskazuje potrzebę budowy lub modernizacji aplikacji VTT, aplikacji hydrometeorologicznej, portalu internetowego RIS oraz aplikacji przeznaczonej do zarządzania usługami i sensorami systemu RIS. Oznacza to, że rozbudowa nie może ograniczać się do dodania nowych lokalizacji terenowych, lecz ma objąć także modernizację warstwy aplikacyjnej, zarządczej i diagnostycznej systemu.

1.1.1.3. Zakres terytorialny

Zakres terytorialny projektu obejmuje zasadniczy obszar rozbudowy systemu RIS na odcinku Odrzańskiej Drogi Wodnej od mostu drogowego DK36 w Ścinawie, tj. km 331,87 rzeki Odry, do mostu drogowego DK40 nad Odrą w Koźlu, tj. km 93,79 rzeki Odry.

Zakres ten obejmuje również istotne odgałęzienia dróg wodnych oraz powiązane funkcjonalnie odcinki infrastruktury żeglugowej, w szczególności Kanał Nawigacyjny we Wrocławiu, Boczny szlak żeglugowy we Wrocławiu, odcinki Odry Południowej i Odry Północnej w rejonie Wrocławia, Kanał śluzy Opatowice, Boczny kanał śluzy Oławy Małej, Kanał śluzy Krapkowice oraz Boczny

kanał śluzy Krapkowice. Łączna długość dróg wodnych analizowanych w zasadniczym obszarze rozbudowy wynosi 272,53 km.

Zakres terytorialny projektu nie ogranicza się jednak wyłącznie do ciągłego odcinka Odry od Ścinawy do Koźla. W ramach przedsięwzięcia przewiduje się również realizację punktowych zadań inwestycyjnych oraz modernizacyjnych na obszarze aktualnie funkcjonującego systemu RIS Dolnej Odry. Dotyczy to w szczególności nowych lokalizacji systemu monitoringu wizyjnego CCTV, których zadaniem jest uzupełnienie możliwości obserwacji miejsc istotnych z punktu widzenia bezpieczeństwa ruchu żeglugowego, nadzoru nad drogą wodną, ochrony infrastruktury technicznej RIS oraz zapewnienia spójności funkcjonalnej systemu na obszarze jego dotychczasowego działania.

W zakresie obecnego obszaru działania systemu RIS Dolnej Odry projekt obejmuje również zadania związane z modernizacją, rozbudową, wymianą, doposażeniem lub dostosowaniem istniejących zasobów infrastrukturalnych, technicznych, transmisyjnych, systemowych i aplikacyjnych systemu RIS, o ile wynika to z zakresu przedmiotu zamówienia, dokumentacji PFU, planów branżowych, dokumentacji projektowej lub przyjętej przez Zamawiającego koncepcji realizacji inwestycji. Zadania te mają charakter uzupełniający i integracyjny wobec zasadniczej rozbudowy terytorialnej systemu RIS na Odrzańskiej Drodze Wodnej.

W ujęciu funkcjonalnym lokalizacje objęte projektem są rozpatrywane nie tylko jako punkty instalacji urządzeń, lecz jako elementy zintegrowanego systemu usług RIS. Dla każdej lokalizacji należy określić jej funkcję w systemie, typ obiektu, zakres planowanych urządzeń lub prac, wymagania transmisyjne, wymagania zasilania, uwarunkowania montażowe, dostępność serwisową, możliwość zabezpieczenia przed dostępem osób nieuprawnionych oraz możliwość uzyskania wymaganych uzgodnień, zgód, decyzji lub warunków technicznych od właścicieli albo zarządców nieruchomości, obiektów lub infrastruktury.

Szczególnego znaczenia nabiera Wrocławski Węzeł Wodny. Jest to obszar o dużej koncentracji dróg wodnych, budowli hydrotechnicznych, mostów i infrastruktury miejskiej, a jednocześnie obszar o istotnym znaczeniu operacyjnym dla żeglugi oraz administracji drogi wodnej. Wdrożenie RIS w tym obszarze powinno zapewniać zarówno obserwację miejsc istotnych dla bezpieczeństwa ruchu, jak i pozyskiwanie danych hydrologicznych oraz meteorologicznych niezbędnych do właściwej oceny warunków nawigacyjnych.

Zakres terytorialny projektu należy zatem rozumieć dwupoziomowo. Pierwszy poziom obejmuje zasadniczy obszar rozbudowy systemu RIS na Odrzańskiej Drodze Wodnej od Ścinawy do Koźla wraz z powiązanymi odgałęzieniami dróg wodnych. Drugi poziom obejmuje punktowe lokalizacje oraz zadania modernizacyjne realizowane na obszarze aktualnie działającego systemu RIS Dolnej Odry, w zakresie niezbędnym do zapewnienia spójności technicznej, funkcjonalnej, transmisyjnej i eksploatacyjnej całego systemu RIS.

Na etapie projektowania Generalny Wykonawca ma obowiązek przeprowadzić weryfikację terenową lokalizacji wskazanych w PFU oraz jego załącznikach, w tym lokalizacji znajdujących się w zasadniczym obszarze rozbudowy oraz lokalizacji punktowych położonych na obszarze obecnie działającego systemu RIS Dolnej Odry. Weryfikacja powinna obejmować co najmniej możliwość montażu urządzeń, warunki konstrukcyjne, warunki zasilania, uwarunkowania środowiskowe, dostępność transmisji danych, możliwość zapewnienia dostępu serwisowego, możliwość zabezpieczenia infrastruktury przed dostępem osób nieuprawnionych, możliwość

uzyskania ostatecznych zgód na montaż infrastruktury na podstawie opracowanej dokumentacji projektowej i innych dokumentów wymaganych przez zarządców obiektów oraz zgodność lokalizacji z wymaganiami funkcjonalnymi systemu RIS.

W przypadku lokalizacji istniejących, modernizowanych albo wykorzystywanych ponownie Generalny Wykonawca ma obowiązek zweryfikować aktualny stan techniczny, formalny i eksploatacyjny zasobów, które mają być objęte realizacją przedmiotu zamówienia. Weryfikacja ta powinna obejmować w szczególności możliwość wykorzystania istniejącej infrastruktury, konieczność jej dostosowania lub wymiany, ograniczenia wynikające z warunków lokalnych oraz wpływ planowanych prac na ciągłość działania obecnego systemu RIS.

1.1.1.4. Zakres rzeczowy inwestycji

Zakres rzeczowy inwestycji obejmuje dziewięć głównych grup zadań:

1) realizację obiektów wieżowych stacji radiokomunikacyjnych VHF/AIS wraz z niezbędną infrastrukturą towarzyszącą, w tym elementami systemów antenowych, urządzeniami radiokomunikacyjnymi, urządzeniami transmisji danych, zasilaniem, zabezpieczeniami technicznymi oraz o ile wynika to z przyjętego rozwiązania projektowego, czujnikami meteorologicznymi i elementami monitoringu wizyjnego instalowanymi na tych obiektach;
2) realizację punktów monitoringu wizyjnego oraz punktów pomiarowych na obiektach mostowych, słupach kamerowych lub innych konstrukcjach wsporczych dopuszczonych do wykorzystania w dokumentacji projektowej, wraz z niezbędnymi kamerami, stacjami czujników hydrologicznych, wyposażeniem teletechnicznym, transmisją danych, zasilaniem oraz elementami montażowymi i zabezpieczającymi;
3) modernizację, rozbudowę, wymianę, doposażenie lub dostosowanie eksploatowanych obecnie urządzeń, instalacji, komponentów, aplikacji i konfiguracji systemu RIS, w zakresie wynikającym z PFU, planów branżowych, dokumentacji projektowej oraz zatwierdzonej koncepcji realizacji inwestycji;
4) doposażenie serwerowni głównej systemu RIS, w tym dostawę, instalację, konfigurację i uruchomienie niezbędnych zasobów infrastruktury serwerowej, pamięci masowej, systemów kopii zapasowych, urządzeń sieciowych, systemów bezpieczeństwa, licencji oraz oprogramowania systemowego i narzędziowego;
5) modernizację pomieszczenia serwerowni pełniącej rolę węzła telekomunikacyjnego systemu RIS, w zakresie niezbędnym do zapewnienia właściwych warunków technicznych, środowiskowych, zasilania, bezpieczeństwa, monitoringu i eksploatacji infrastruktury teleinformatycznej;
6) modernizację sieci teleinformatycznej w siedzibie Zamawiającego, w zakresie niezbędnym do obsługi rozbudowanego systemu RIS, zapewnienia bezpiecznej komunikacji, segmentacji ruchu, monitoringu, zarządzania, integracji z istniejącą infrastrukturą oraz utrzymania wymaganej dostępności usług;
7) utworzenie serwerowni zapasowej, jej wyposażenie, uruchomienie oraz połączenie z siedzibą Zamawiającego światłowodowym łączem telekomunikacyjnym lub innym rozwiązaniem transmisyjnym zaakceptowanym przez Zamawiającego, zapewniającym wymagany poziom dostępności, bezpieczeństwa, przepustowości i redundancji;

8) opracowanie, wdrożenie, integrację i uruchomienie usług cyfrowych systemu RIS, w tym usług, modułów, interfejsów, mechanizmów wymiany danych, funkcji operatorskich, administracyjnych, raportowych, monitorujących i integracyjnych wymaganych dla prawidłowego funkcjonowania systemu;

9) modernizację architektury systemu RIS, obejmującą dostosowanie usług cyfrowych, komponentów integracyjnych, infrastruktury technicznej, mechanizmów wymiany danych oraz środowisk systemowych do wymagań interoperacyjności, współpracy z systemami krajowymi i europejskimi oraz włączenia krajowej administracji żeglugi śródlądowej do struktur i usług europejskich właściwych dla RIS.

1.1.1.5. Miejsce realizacji przedmiotu zamówienia

Przedmiot zamówienia będzie realizowany w:

- siedzibie Centrum RIS znajdującej się w siedzibie Urzędu Żeglugi Śródlądowej w Szczecinie,
- siedzibie zewnętrznego Data Center w którym ma zostać utworzona serwerownia zapasowa systemu RIS,
- siedzibie Urzędu Żeglugi Śródlądowej we Wrocławiu oraz jego delegaturze terenowej w Kędzierzynie-Koźlu,
- istniejących oraz nowych lokalizacjach obiektów infrastruktury systemu RIS danego typu.

1.1.1.5.1. Obiekty wieżowe stacji radiokomunikacyjnych VHF/AIS, czujników meteorologicznych oraz kamer monitoringu wizyjnego

W zakresie rozbudowy systemu RIS na Odrzańskiej Drodze wodnej ma powstać 8 nowych wież radiowych stacji radiokomunikacyjnych VHF/AIS wraz z funkcją DGNSS, czujników meteorologicznych oraz kamer obserwacyjnych i dozorowych.

Założenia rozbudowy systemu łączności radiowej VHF/AIS zawarto w załączniku do PFU pt.: „Plan łączności radiowej VHF/AIS”.

Zakres tego zadania w zakresie instalacji kamer obserwacyjnych i dozorowych w lokalizacjach posadowienia wież antenowych ujęto w załączniku do PFU pt.: „Plan systemu monitoringu wizyjnego (CCTV)”.

Tabela 1: Wykaz nowych wież antenowych stacji radiokomunikacyjnych VHF/AIS wraz z funkcją DGNSS, czujników meteorologicznych oraz kamer obserwacyjnych i dozorowych

Lp.	Nazwa	Uwagi	Zarządca
1.	Ścinawa	Samonośna wieża kratownicowa stalowa o wysokości co najmniej 32 m powiększonej o zwód pionowy instalacji piorunochronnej, wyniesiony ponad najwyżej położone elementy antenowe i konstrukcyjne wieży.	Urząd Miasta i Gminy w Ścinawie

Lp.	Nazwa	Uwagi	Zarządca
2.	Brzeg Dolny	Samonośna wieża kratownicowa stalowa o wysokości co najmniej 32 m powiększonej o zwód pionowy instalacji piorunochronnej, wyniesiony ponad najwyżej położone elementy antenowe i konstrukcyjne wieży. Teren obiektu hydrotechnicznego: Stopień wodny Brzeg Dolny.	PGW Wody Polskie, RZGW Wrocław, Zarząd Zlewni w Lesznie
3.	Wrocław Rędzin	Samonośna wieża kratownicowa stalowa o wysokości co najmniej 32 m powiększonej o zwód pionowy instalacji piorunochronnej, wyniesiony ponad najwyżej położone elementy antenowe i konstrukcyjne wieży. Teren obiektu hydrotechnicznego: Stopień wodny Rędzin. Zadanie obejmuje demontaż istniejącej wieży antenowej RZGW wraz z przewieszeniem zawieszonych tam anten na nową wieżę radiową.	PGW Wody Polskie, RZGW Wrocław, Zarząd Zlewni we Wrocławiu
4.	Wrocław Szczytniki	Samonośna wieża kratownicowa stalowa o wysokości co najmniej 42 m powiększonej o zwód pionowy instalacji piorunochronnej, wyniesiony ponad najwyżej położone elementy antenowe i konstrukcyjne wieży. Teren obiektu hydrotechnicznego: Śluza Szczytniki, Wyspa Szczytniki.	PGW Wody Polskie, RZGW Wrocław, Zarząd Zlewni we Wrocławiu
5.	Wrocław Bartoszewice	Samonośna wieża kratownicowa stalowa o wysokości co najmniej 32 m powiększonej o zwód pionowy instalacji piorunochronnej, wyniesiony ponad najwyżej położone elementy antenowe i konstrukcyjne wieży. Teren obiektu hydrotechnicznego: Stopień wodny Bartoszewice. Zadanie obejmuje demontaż istniejącej wieży antenowej RZGW wraz z przewieszeniem zawieszonych tam anten na nową wieżę radiową.	PGW Wody Polskie, RZGW Wrocław, Zarząd Zlewni we Wrocławiu
6.	Brzeg	Nowa wieża antenowa o wysokości co najmniej 32 m. Teren obiektu hydrotechnicznego: Stopień wodny Brzeg.	PGW Wody Polskie, RZGW Wrocław, Zarząd Zlewni we Wrocławiu
7.	Opole	Samonośna wieża kratownicowa stalowa o wysokości co najmniej 42 m powiększonej o zwód pionowy instalacji piorunochronnej, wyniesiony ponad najwyżej położone elementy antenowe i konstrukcyjne wieży. Teren nieczynnej stoczni rzecznej na wyspie Pasieka.	PGW Wody Polskie, RZGW Gliwice, Zarząd Zlewni w Opolu

Lp.	Nazwa	Uwagi	Zarządca
		Teren PGW Wody Polskie – Nadzór Wodny Opole, ul. Jana Kochanowskiego 9, identyfikator działki 166101_1.0103.56/10. Budowa nowej wieży antenowej ma być realizowana w reżimie wytycznych oraz uzgodnień Opolskiego Wojewódzkiego Konserwatora Zabytków, który wymaga zastosowania stonowanej kolorystyki obiektu, bez użycia jaskrawych barw takich jak czerwień oraz zachowania odpowiedniego dystansu od historycznej zabudowy.	
8.	Kędzierzyn-Koźle	Samonośna wieża kratownicowa stalowa o wysokości co najmniej 32 m powiększonej o zwód pionowy instalacji piorunochronnej, wyniesiony ponad najwyżej położone elementy antenowe i konstrukcyjne wieży. Teren obiektu Hydrotechnicznego Jaz Koźle, ul. Wyspa 20, 47-200 Kędzierzyn-Koźle, identyfikator działki: 160301_1.0014.2477/15 znajdującej się w pobliżu lądowiska przyszpitalnego H328. Wieża musi posiadać oznakowanie przeszkodowe dzienne i nocne, zgodne z rozporządzeniem Ministra Infrastruktury w sprawie przeszkód lotniczych, powierzchni ograniczających przeszkody oraz urządzeń o charakterze niebezpiecznym[1] Zadanie obejmuje demontaż istniejącej wieży antenowej RZGW wraz z przewieszeniem zawieszonych tam anten na nową wieżę radiową.	PGW Wody Polskie, RZGW Gliwice, Zarząd Zlewni w Gliwicach

1.1.1.5.2. Punkty monitoringu wizyjnego oraz stacji czujników hydrologicznych

W zakresie rozbudowy systemu RIS na Odrzańskiej Drodze wodnej ma powstać 27 nowych lokalizacji monitoringu wizyjnego, w tym 8 stacji czujników hydrologicznych.

Powyższa tabele nie ujmuje funkcji obserwacyjnej lokalizacji obiektów wieżowych wymienionych w poprzedniej jednostce redakcyjnej dokumentu.

[1] https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20250000903

Tabela 2: Wykaz nowych lokalizacji monitoringu wizyjnego oraz stacji czujników hydrologicznych

Lp.	Nazwa	Funkcja obserwacyjna	Funkcja pomiarów hydrologicznych	Zarządca
1.	Szczecin - Wyspa Bielawa (Wyspa Grodzka)	✓		Żegluga Szczecińska Turystyka Wydarzenia Sp. z o.o.
2.	Szczecin Podjuchy – Most kolejowy im. dr inż. Andrzeja Krefta	✓	✓	PKP Polskie Linie Kolejowe S.A. - Zakład Linii Kolejowych w Szczecinie
3.	Siekierki – Kładka pieszo-rowerowa na Odrze	✓		Amt Barnim-Oderbruch
4.	Kostrzyn nad Odrą - Most kolejowy nr 2 na Warcie (Linia nr 273)	✓		PKP Polskie Linie Kolejowe S.A. - Zakład Linii Kolejowych w Zielonej Górze
5.	Kostrzyn nad Odrą - Most drogowy na Warcie (DK 31)	✓		Generalna Dyrekcja Dróg Krajowych i Autostrad Oddział Zielona Góra
6.	Ścinawa	✓		Urząd Miasta i Gminy Ścinawa
7.	Ścinawa - Most drogowy (DK 36)	✓	✓	Generalna Dyrekcja Dróg Krajowych i Autostrad Oddział we Wrocławiu
8.	Ścinawa - Most kolejowy (LK273)	✓		PKP Polskie Linie Kolejowe S.A. - Zakład Linii Kolejowych we Wrocławiu
9.	Brzeg Dolny - teren stopnia wodnego Brzeg Dolny, śluza Brzeg Dolny	✓		PGW Wody Polskie, Zarząd Zlewni we Wrocławiu
10.	Wrocław Rędzin - teren stopnia wodnego Rędzin, śluza Rędzin	✓		PGW Wody Polskie, Zarząd Zlewni we Wrocławiu
11.	Wrocław Osobowice - Most Milenijny (DK 5)	✓	✓	Zarząd Dróg i Utrzymania Miasta we Wrocławiu
12.	Wrocław Osobowice - Most kolejowy (LK 271)	✓		Zakład Linii Kolejowych we Wrocławiu
13.	Wrocław Piasek - Most Pokoju	✓		Zarząd Dróg i Utrzymania Miasta we Wrocławiu
14.	Wrocław Piasek - Most Grunwaldzki (DW 372)	✓	✓	Zarząd Dróg i Utrzymania Miasta we Wrocławiu
15.	Wrocław Szczytniki - teren śluzy Szczytniki (Wyspa Szczytniki)	✓		PGW Wody Polskie, Zarząd Zlewni we Wrocławiu
16.	Wrocław Dąbie - Kładka Zwierzyniecka	✓		Zarząd Dróg i Utrzymania Miasta we Wrocławiu

Lp.	Nazwa	Funkcja obserwacyjna	Funkcja pomiarów hydrologicznych	Zarządca
17.	Wrocław Dąbie - Most Olimpijski	✓		Zarząd Dróg i Utrzymania Miasta we Wrocławiu
18.	Wrocław Bartoszowice – teren stopnia wodnego Bartoszowice, śluza Bartoszowice	✓		PGW Wody Polskie, Zarząd Zlewni we Wrocławiu
19.	Brzeg – teren stopnia wodnego Brzeg	✓		PGW Wody Polskie, Zarząd Zlewni we Wrocławiu
20.	Opole Północ - Most Pamięci Sybiraków (DW 435)	✓	✓	Miejski Zarząd Dróg w Opolu
21.	Opole Centrum - Most kolejowy (LK 132)	✓		PKP Polskie Linie Kolejowe S.A. - Zakład Linii Kolejowych w Opolu
22.	Opole Południe - Most im. Ireny Sendlerowej	✓		Miejski Zarząd Dróg w Opolu
23.	Opole - teren nieczynnej stoczni rzecznej na wyspie Pasieka, teren PGW Wody Polskie – Nadzór Wodny Opole, ul. Jana Kochanowskiego 9	✓		PGW Wody Polskie, Zarząd Zlewni w Opolu
24.	Krapkowice - Most drogowy (DW 409) w ciągu ul. Księdza Koziołka	✓	✓	Zarząd Dróg Wojewódzkich w Opolu
25.	Kłodnica Północ - Most drogowy (DW 423) w ciągu ulicy Kłodnickiej	✓	✓	Zarząd Dróg Wojewódzkich w Opolu
26.	Koźle Południe - Most drogowy Józefa Długosza	✓	✓	Urząd Miasta Kędzierzyn-Koźle
27.	Koźle Południe Ostrówek - teren obiektu Hydrotechnicznego Jaz Koźle, ul. Wyspa 20, 47-200 Kędzierzyn-Koźle	✓		PGW Wody Polskie, Zarząd Zlewni w Opolu

1.1.1.5.3. Obiekty wymiany obecnych urządzeń i elementów systemu RIS

Działania o charakterze modernizacyjno-odtworzeniowym obejmujące wymianę wybranych obecnie eksploatowanych urządzeń i elementów funkcjonującego systemu RIS dotyczy infrastruktury terenowej eksploatowanej w 36 lokalizacjach.

Tabela 3: Wykaz obiektów infrastruktury systemu RIS objętych wymianą obecnych urządzeń i elementów

Lp.	Nazwa	Zakres modernizacyjno-odtworzeniowy
1.	Szczecin – Elewator EWA	1. Demontaż dwóch zasilaczy awaryjnych UPS PowerWalker VI 1000 RT HID. 2. Montaż dwóch zasilaczy awaryjnych QUINT-UPS/1AC/1AC/500VA wraz z modułem bateryjnym UPS-BAT/VRLA-WTR/24DC/13AH albo rozwiązanie równoważne o parametrach nie gorszych, zaakceptowane przez Zamawiającego. 3. Montaż przełącznika zasilania awaryjnego wraz z włączeniem go do układu zasilania szafy teletechnicznej. 4. Wymiana kamery PTZ na nową.
2.	Szczecin – Most Długi	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA. 2. Dostawa, instalacja i wdrożenie rozwiązania sprzętowo-aplikacyjnego tzw. lokalnego komponent akwizycji, przetwarzania, buforowania i transmisji danych pomiarowych, umożliwiający obsługę zastosowanych czujników, rejestrację odczytów, kontrolę poprawności danych, przekazywanie danych do Centrum RIS oraz zachowanie ciągłości rejestracji pomiarów w przypadku czasowej utraty połączenia transmisyjnego z Centrum RIS (obsługa wodowskazów).
3.	Szczecin – pl. Batorego 4	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA. 2. Wymiana kamery PTZ na nową.
4.	Szczecin – Most kolejowy Dworzec Główny	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA. 2. Dostawa, instalacja i wdrożenie rozwiązania sprzętowo-aplikacyjnego tzw. lokalnego komponent akwizycji, przetwarzania, buforowania i transmisji danych pomiarowych, umożliwiający obsługę zastosowanych czujników, rejestrację odczytów, kontrolę poprawności danych, przekazywanie danych do Centrum RIS

Lp.	Nazwa	Zakres modernizacyjno-odtworzeniowy
		oraz zachowanie ciągłości rejestracji pomiarów w przypadku czasowej utraty połączenia transmisyjnego z Centrum RIS (obsługa wodowskazów).
5.	Szczecin – Most Portowy	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA. 2. Dostawa, instalacja i wdrożenie rozwiązania sprzętowo-aplikacyjnego tzw. lokalnego komponent akwizycji, przetwarzania, buforowania i transmisji danych pomiarowych, umożliwiający obsługę zastosowanych czujników, rejestrację odczytów, kontrolę poprawności danych, przekazywanie danych do Centrum RIS oraz zachowanie ciągłości rejestracji pomiarów w przypadku czasowej utraty połączenia transmisyjnego z Centrum RIS (obsługa wodowskazów).
6.	Szczecin – Most kolejowy Parnica	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA. 2. Dostawa, instalacja i wdrożenie rozwiązania sprzętowo-aplikacyjnego tzw. lokalnego komponent akwizycji, przetwarzania, buforowania i transmisji danych pomiarowych, umożliwiający obsługę zastosowanych czujników, rejestrację odczytów, kontrolę poprawności danych, przekazywanie danych do Centrum RIS oraz zachowanie ciągłości rejestracji pomiarów w przypadku czasowej utraty połączenia transmisyjnego z Centrum RIS (obsługa wodowskazów).
7.	Szczecin – ul. Potulicka 40	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA. 2. Wymiana kamery stacjonarnej z widokiem w kierunku Wyspy Zielonej (S) na nową. 3. Dostawa, instalacja i wdrożenie rozwiązania sprzętowo-aplikacyjnego tzw. lokalnego komponent akwizycji, przetwarzania, buforowania i transmisji danych pomiarowych, umożliwiający obsługę zastosowanych czujników, rejestrację odczytów, kontrolę poprawności danych, przekazywanie danych do Centrum RIS oraz zachowanie ciągłości rejestracji pomiarów w przypadku czasowej utraty połączenia transmisyjnego z Centrum RIS (obsługa stacji meteorologicznej).

Lp.	Nazwa	Zakres modernizacyjno-odtworzeniowy
8.	Szczecin (Port) – teren ZMPSiŚ	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA. 2. Dostawa, instalacja i wdrożenie rozwiązania sprzętowo-aplikacyjnego tzw. lokalnego komponent akwizycji, przetwarzania, buforowania i transmisji danych pomiarowych, umożliwiający obsługę zastosowanych czujników, rejestrację odczytów, kontrolę poprawności danych, przekazywanie danych do Centrum RIS oraz zachowanie ciągłości rejestracji pomiarów w przypadku czasowej utraty połączenia transmisyjnego z Centrum RIS (obsługa stacji meteorologicznej).
9.	Szczecin – Most Pionierów	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA. 2. Dostawa, instalacja i wdrożenie rozwiązania sprzętowo-aplikacyjnego tzw. lokalnego komponent akwizycji, przetwarzania, buforowania i transmisji danych pomiarowych, umożliwiający obsługę zastosowanych czujników, rejestrację odczytów, kontrolę poprawności danych, przekazywanie danych do Centrum RIS oraz zachowanie ciągłości rejestracji pomiarów w przypadku czasowej utraty połączenia transmisyjnego z Centrum RIS (obsługa wodowskazów).
10.	Szczecin – Most Pomorzan (kolejowy – strona północna)	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA.
11.	Szczecin – Most Pomorzan (drogowy – strona południowa)	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA.
12.	Szczecin – Most Gryfitów (kolejowy – strona północna)	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA. 2. Dostawa, instalacja i wdrożenie rozwiązania sprzętowo-aplikacyjnego tzw. lokalnego komponent akwizycji, przetwarzania, buforowania i transmisji danych pomiarowych, umożliwiający obsługę zastosowanych czujników, rejestrację odczytów, kontrolę poprawności danych, przekazywanie danych do Centrum RIS

Lp.	Nazwa	Zakres modernizacyjno-odtworzeniowy
		oraz zachowanie ciągłości rejestracji pomiarów w przypadku czasowej utraty połączenia transmisyjnego z Centrum RIS (obsługa wodowskazów).
13.	Szczecin – Most Gryfitów (drogowy – strona południowa)	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA.
14.	Podjuchy – Wieża na terenie placówki RZGW	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA. 2. Wymiana kamery PTZ na nową. 3. Wymiana kamery stacjonarnej z widokiem na lodołamacze na nową.
15.	Siadło Górne	1. Demontaż zasilacza awaryjnego UPS PowerWalker VI 1000 RT HID oraz jego modułów bateryjnych. 2. Montaż dwóch zasilaczy awaryjnych QUINT-UPS/1AC/1AC/500VA wraz z modułem bateryjnym UPS-BAT/VRLA-WTR/24DC/13AH albo rozwiązanie równoważne o parametrach nie gorszych, zaakceptowane przez Zamawiającego. 3. Montaż przełącznika zasilania awaryjnego wraz z włączeniem go do układu zasilania szafy teletechnicznej. 4. Demontaż starej kamery dozorowej.
16.	Most Autostradowy A6 – Zachód	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA.
17.	Most Autostradowy A6 – Wschód	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA.
18.	Mescherin – Most drogowy	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA. 2. Dostawa, instalacja i wdrożenie rozwiązania sprzętowo-aplikacyjnego tzw. lokalnego komponent akwizycji, przetwarzania, buforowania i transmisji danych pomiarowych, umożliwiający obsługę zastosowanych czujników, rejestrację odczytów, kontrolę poprawności danych, przekazywanie danych do Centrum RIS

Lp.	Nazwa	Zakres modernizacyjno-odtworzeniowy
		oraz zachowanie ciągłości rejestracji pomiarów w przypadku czasowej utraty połączenia transmisyjnego z Centrum RIS (obsługa wodowskazów).
19.	Gryfino – Most drogowy	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA. 2. Wymiana kamery PTZ na nową. 3. Dostawa, instalacja i wdrożenie rozwiązania sprzętowo-aplikacyjnego tzw. lokalnego komponent akwizycji, przetwarzania, buforowania i transmisji danych pomiarowych, umożliwiający obsługę zastosowanych czujników, rejestrację odczytów, kontrolę poprawności danych, przekazywanie danych do Centrum RIS oraz zachowanie ciągłości rejestracji pomiarów w przypadku czasowej utraty połączenia transmisyjnego z Centrum RIS (obsługa wodowskazów oraz stacji meteorologicznej).
20.	Gryfino – Most drogowy	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA.
21.	Widuchowa – Jaz	1. Demontaż dwóch zasilaczy awaryjnych UPS PowerWalker VI 1000 RT HID. 2. Montaż dwóch zasilaczy awaryjnych QUINT-UPS/1AC/1AC/500VA wraz z modułem bateryjnym UPS-BAT/VRLA-WTR/24DC/13AH albo rozwiązanie równoważne o parametrach nie gorszych, zaakceptowane przez Zamawiającego. 3. Montaż przełącznika zasilania awaryjnego wraz z włączeniem go do układu zasilania szafy teletechnicznej. 4. Demontaż niesprawnego agregatu prądotwórczego wraz z jego instalacją elektryczną; 5. Wykonanie niezależnego od PGW Wody Polskie przyłącza energetycznego umożliwiającego samodzielne rozliczanie zużycia energii elektrycznej z operatorem systemu dystrybucyjnego. 6. Dostawa, instalacja i wdrożenie rozwiązania sprzętowo-aplikacyjnego tzw. lokalnego komponent akwizycji, przetwarzania, buforowania i transmisji danych

Lp.	Nazwa	Zakres modernizacyjno-odtworzeniowy
		pomiarowych, umożliwiający obsługę zastosowanych czujników, rejestrację odczytów, kontrolę poprawności danych, przekazywanie danych do Centrum RIS oraz zachowanie ciągłości rejestracji pomiarów w przypadku czasowej utraty połączenia transmisyjnego z Centrum RIS (obsługa stacji meteorologicznej).
22.	Ognica – Wieża na terenie nabrzeża RZGW	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA.
23.	Krajnik Dolny – Most drogowy na Odrze (DK 26)	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA. 2. Dostawa, instalacja i wdrożenie rozwiązania sprzętowo-aplikacyjnego tzw. lokalnego komponent akwizycji, przetwarzania, buforowania i transmisji danych pomiarowych, umożliwiający obsługę zastosowanych czujników, rejestrację odczytów, kontrolę poprawności danych, przekazywanie danych do Centrum RIS oraz zachowanie ciągłości rejestracji pomiarów w przypadku czasowej utraty połączenia transmisyjnego z Centrum RIS (obsługa wodowskazów). 3. Zmiana montażu kamery patrzącej w kierunku północnym eliminująca widok przęsła mostu.
24.	Bielinek	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA. 2. Demontaż zasilacza awaryjnego UPS PowerWalker VI 1000 RT HID. 3. Montaż zasilacza awaryjnego QUINT-UPS/1AC/1AC/500VA wraz z modułem bateryjnym UPS-BAT/VRLA-WTR/24DC/13AH albo rozwiązanie równoważne o parametrach nie gorszych, zaakceptowane przez Zamawiającego. 4. Dostawa, instalacja i wdrożenie rozwiązania sprzętowo-aplikacyjnego tzw. lokalnego komponent akwizycji, przetwarzania, buforowania i transmisji danych pomiarowych, umożliwiający obsługę zastosowanych czujników, rejestrację odczytów, kontrolę poprawności danych, przekazywanie danych do Centrum RIS

Lp.	Nazwa	Zakres modernizacyjno-odtworzeniowy
		oraz zachowanie ciągłości rejestracji pomiarów w przypadku czasowej utraty połączenia transmisyjnego z Centrum RIS (obsługa stacji meteorologicznej).
25.	Bielinek - Kopalnia Bielinek Nabrzeże (Stacja pomp)	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA. 2. Dostawa, instalacja i wdrożenie rozwiązania sprzętowo-aplikacyjnego tzw. lokalnego komponent akwizycji, przetwarzania, buforowania i transmisji danych pomiarowych, umożliwiający obsługę zastosowanych czujników, rejestrację odczytów, kontrolę poprawności danych, przekazywanie danych do Centrum RIS oraz zachowanie ciągłości rejestracji pomiarów w przypadku czasowej utraty połączenia transmisyjnego z Centrum RIS (obsługa wodowskazów).
26.	Osinów Dolny – Most drogowy na Odrze	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA. 2. Dostawa, instalacja i wdrożenie rozwiązania sprzętowo-aplikacyjnego tzw. lokalnego komponent akwizycji, przetwarzania, buforowania i transmisji danych pomiarowych, umożliwiający obsługę zastosowanych czujników, rejestrację odczytów, kontrolę poprawności danych, przekazywanie danych do Centrum RIS oraz zachowanie ciągłości rejestracji pomiarów w przypadku czasowej utraty połączenia transmisyjnego z Centrum RIS (obsługa wodowskazów).
27.	Siekierki - Most kolejowy na Odrze	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA. 2. Dostawa, instalacja i wdrożenie rozwiązania sprzętowo-aplikacyjnego tzw. lokalnego komponent akwizycji, przetwarzania, buforowania i transmisji danych pomiarowych, umożliwiający obsługę zastosowanych czujników, rejestrację odczytów, kontrolę poprawności danych, przekazywanie danych do Centrum RIS oraz zachowanie ciągłości rejestracji pomiarów w przypadku czasowej utraty połączenia transmisyjnego z Centrum RIS (obsługa wodowskazów).

Lp.	Nazwa	Zakres modernizacyjno-odtworzeniowy
28.	Gozdowice – Nadzór Wodny RZGW	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA. 2. Demontaż zasilacza awaryjnego UPS PowerWalker VI 1000 RT HID. 3. Montaż zasilacza awaryjnego QUINT-UPS/1AC/1AC/500VA wraz z modułem bateryjnym UPS-BAT/VRLA-WTR/24DC/13AH albo rozwiązanie równoważne o parametrach nie gorszych, zaakceptowane przez Zamawiającego. 4. Dostawa, instalacja i wdrożenie rozwiązania sprzętowo-aplikacyjnego tzw. lokalnego komponent akwizycji, przetwarzania, buforowania i transmisji danych pomiarowych, umożliwiający obsługę zastosowanych czujników, rejestrację odczytów, kontrolę poprawności danych, przekazywanie danych do Centrum RIS oraz zachowanie ciągłości rejestracji pomiarów w przypadku czasowej utraty połączenia transmisyjnego z Centrum RIS (obsługa stacji meteorologicznej).
29.	Gozdowice - Nabrzeże	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA. 2. Dostawa, instalacja i wdrożenie rozwiązania sprzętowo-aplikacyjnego tzw. lokalnego komponent akwizycji, przetwarzania, buforowania i transmisji danych pomiarowych, umożliwiający obsługę zastosowanych czujników, rejestrację odczytów, kontrolę poprawności danych, przekazywanie danych do Centrum RIS oraz zachowanie ciągłości rejestracji pomiarów w przypadku czasowej utraty połączenia transmisyjnego z Centrum RIS (obsługa wodowskazów).
30.	Świerkocin – Nadzór Wodny RZGW	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA. 2. Demontaż zasilacza awaryjnego UPS PowerWalker VI 1000 RT HID. 3. Montaż zasilacza awaryjnego QUINT-UPS/1AC/1AC/500VA wraz z modułem bateryjnym UPS-BAT/VRLA-WTR/24DC/13AH albo rozwiązanie równoważne o parametrach nie gorszych, zaakceptowane przez Zamawiającego.

Lp.	Nazwa	Zakres modernizacyjno-odtworzeniowy
		4. Dostawa, instalacja i wdrożenie rozwiązania sprzętowo-aplikacyjnego tzw. lokalnego komponent akwizycji, przetwarzania, buforowania i transmisji danych pomiarowych, umożliwiający obsługę zastosowanych czujników, rejestrację odczytów, kontrolę poprawności danych, przekazywanie danych do Centrum RIS oraz zachowanie ciągłości rejestracji pomiarów w przypadku czasowej utraty połączenia transmisyjnego z Centrum RIS (obsługa wodowskazów oraz stacji pogodowej).
31.	Kostrzyn nad Odrą - Most kolejowy nr 2 na Warcie (Linia nr 273)	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA. 2. Dostawa, instalacja i wdrożenie rozwiązania sprzętowo-aplikacyjnego tzw. lokalnego komponent akwizycji, przetwarzania, buforowania i transmisji danych pomiarowych, umożliwiający obsługę zastosowanych czujników, rejestrację odczytów, kontrolę poprawności danych, przekazywanie danych do Centrum RIS oraz zachowanie ciągłości rejestracji pomiarów w przypadku czasowej utraty połączenia transmisyjnego z Centrum RIS (obsługa wodowskazów).
32.	Kostrzyn nad Odrą - Most drogowy na Warcie (DK 31)	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA. 2. Dostawa, instalacja i wdrożenie rozwiązania sprzętowo-aplikacyjnego tzw. lokalnego komponent akwizycji, przetwarzania, buforowania i transmisji danych pomiarowych, umożliwiający obsługę zastosowanych czujników, rejestrację odczytów, kontrolę poprawności danych, przekazywanie danych do Centrum RIS oraz zachowanie ciągłości rejestracji pomiarów w przypadku czasowej utraty połączenia transmisyjnego z Centrum RIS (obsługa wodowskazów).
33.	Kostrzyn nad Odrą – teren Muzeum Twierdzy Kostrzyn nad Odrą	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA. 2. Demontaż zasilacza awaryjnego UPS PowerWalker VI 1000 RT HID.

Lp.	Nazwa	Zakres modernizacyjno-odtworzeniowy
		3. Montaż zasilacza awaryjnego QUINT-UPS/1AC/1AC/500VA wraz z modułem bateryjnym UPS-BAT/VRLA-WTR/24DC/13AH albo rozwiązanie równoważne o parametrach nie gorszych, zaakceptowane przez Zamawiającego. 4. Dostawa, instalacja i wdrożenie rozwiązania sprzętowo-aplikacyjnego tzw. lokalnego komponent akwizycji, przetwarzania, buforowania i transmisji danych pomiarowych, umożliwiający obsługę zastosowanych czujników, rejestrację odczytów, kontrolę poprawności danych, przekazywanie danych do Centrum RIS oraz zachowanie ciągłości rejestracji pomiarów w przypadku czasowej utraty połączenia transmisyjnego z Centrum RIS (obsługa stacji meteorologicznej).
34.	Kostrzyn nad Odrą – Most drogowy nad Odrą	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA. 2. Dostawa, instalacja i wdrożenie rozwiązania sprzętowo-aplikacyjnego tzw. lokalnego komponent akwizycji, przetwarzania, buforowania i transmisji danych pomiarowych, umożliwiający obsługę zastosowanych czujników, rejestrację odczytów, kontrolę poprawności danych, przekazywanie danych do Centrum RIS oraz zachowanie ciągłości rejestracji pomiarów w przypadku czasowej utraty połączenia transmisyjnego z Centrum RIS (obsługa wodowskazów).
35.	Słubice – Most drogowy nad Odrą (DK 29)	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA. 2. Dostawa, instalacja i wdrożenie rozwiązania sprzętowo-aplikacyjnego tzw. lokalnego komponent akwizycji, przetwarzania, buforowania i transmisji danych pomiarowych, umożliwiający obsługę zastosowanych czujników, rejestrację odczytów, kontrolę poprawności danych, przekazywanie danych do Centrum RIS oraz zachowanie ciągłości rejestracji pomiarów w przypadku czasowej utraty połączenia transmisyjnego z Centrum RIS (obsługa wodowskazów).
36.	Słubice – Nadzór Wodny RZGW	1. Wymiana modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA. 2. Demontaż zasilacza awaryjnego UPS PowerWalker VI 1000 RT HID.

Lp.	Nazwa	Zakres modernizacyjno-odtworzeniowy
		3. Montaż zasilacza awaryjnego QUINT-UPS/1AC/1AC/500VA wraz z modułem bateryjnym UPS-BAT/VRLA-WTR/24DC/13AH albo rozwiązanie równoważne o parametrach nie gorszych, zaakceptowane przez Zamawiającego. 4. Dostawa, instalacja i wdrożenie rozwiązania sprzętowo-aplikacyjnego tzw. lokalnego komponent akwizycji, przetwarzania, buforowania i transmisji danych pomiarowych, umożliwiający obsługę zastosowanych czujników, rejestrację odczytów, kontrolę poprawności danych, przekazywanie danych do Centrum RIS oraz zachowanie ciągłości rejestracji pomiarów w przypadku czasowej utraty połączenia transmisyjnego z Centrum RIS (obsługa wodowskazów oraz stacji meteorologicznej).

1.1.1.5.4. Obiekty hydrotechniczne monitorowane na bazie infrastruktury RZGW

W fazie przegotowania projektu Urząd Żeglugi Śródlądowej w Szczecinie w wyniki konsultacji z Departamentem Ochrony Przed Powodzią i Suszą Państwowego Gospodarstwa Wodnego Wody Polskie, Krajowy Zarząd Gospodarki Wodnej uzyskał potwierdzenie możliwości udostępnienia strumieni wideo systemu monitoringu wskazanych budowli hydrotechnicznych będących w zarządzie PGW Wody Polskie:

1) Śluza Malczyce,
2) Śluza Brzeg Dolny,
3) Śluza Rędzin,
4) Śluza Różanka,
5) Śluza Bartoszewice,
6) Śluza Oława,
7) Śluza Brzeg,
8) Śluza stopnia wodnego Ujście Nysy,
9) Śluza Opole.

Zgodnie z ustaleniami każdy z wymienionych obiektów wymaga indywidualnej analizy, a ostateczne zatwierdzenie listy obiektów oraz przekazanie strumieni wideo z poszczególnych kamer będzie wymagało spotkań technicznych Wykonawcy oraz Zamawiającego z pracownikami Wydziału Obsługi Informatycznej Południe PGW Wody Polskie. Celem spotkań technicznych ma być precyzyjne wskazanie, z których kamer zostanie udostępniony sygnał oraz ustalenie metody transmisji sygnału.

Zamawiający przekaże kontakty robocze do pracownikami Wydziału Obsługi Informatycznej Południe Wykonawcy po podpisaniu Umowy.

Zakres tego zadania ujęto w załączniku do PFU pt.: „Plan systemu monitoringu wizyjnego (CCTV)”.

.

1.1.1.5.5. Zbiorcze zestawienie nowych lokalizacji terenowych oraz ich funkcji

W poniższej tabeli przedstawiono zbiorcze zestawienie nowych lokalizacji terenowych systemu RIS przewidzianych do realizacji w ramach przedmiotu zamówienia wraz z przypisaniem ich podstawowych funkcji użytkowych i technicznych. Zestawienie ma charakter syntetyczny i porządkujący. Jego celem jest wskazanie, które lokalizacje będą pełniły funkcję związaną z łącznością radiową VHF/AIS, pomiarem meteorologicznym, pomiarem hydrologicznym oraz obserwacją wizyjną.

Tabela obejmuje lokalizacje, w których przewiduje się realizację nowych obiektów wieżowych, punktów kamerowych, punktów pomiarowych albo innych elementów terenowej infrastruktury systemu RIS. Dla każdej lokalizacji wskazano planowane funkcje, orientacyjną liczbę kamer stałych i kamer PTZ oraz rodzaj obiektu albo platformy nośnej, na której przewiduje się instalację urządzeń.

Zestawienie nie zastępuje szczegółowych opisów zakresu rzeczowego, wymagań technicznych, wymagań instalacyjnych, założeń projektowych, uzgodnień lokalizacyjnych ani dokumentów branżowych stanowiących załączniki do PFU. Szczegółowe wymagania dotyczące poszczególnych podsystemów określają odpowiednie rozdziały PFU oraz dokumenty: „Plan łączności radiowej VHF/AIS”, „Plan systemu monitoringu wizyjnego (CCTV)” oraz „Plan połączeń transmisyjnych”.

Tabela 4: Zbiorcze zestawienie nowych lokalizacji systemu RIS oraz och funkcji

Funkcje
R – Łączność radiowa VHF/AIS
M – Meteorologiczna
H – Hydrologiczna
O – Obserwacyjna

Lp.	Lokalizacja	Funkcje				Kamery stałe	Kamery PTZ	Rodzaj obiektu
		R	M	H	O			
1.	Szczecin - Wyspa Bielawa (Wyspa Grodzka)				✓	1	1	słup kamerowy
2.	Szczecin Podjuchy - Most kolejowy im. dr inż. Andrzeja Krefta			✓	✓	2		obiekt mostowy

Lp.	Lokalizacja	Funkcje				Kamery stałe	Kamery PTZ	Rodzaj obiektu
		R	M	H	O			
3.	Ścinawa **Uwaga:** Numer działki i dokładna lokalizacja punktu kamerowego/wieży radiowej w Ścinawie muszą zostać potwierdzone w dokumentacji projektowej na podstawie aktualnych uzgodnień z właścicielem albo zarządcą nieruchomości.	✓	✓		✓	1	1	wieża
4.	Ścinawa - Most drogowy (DK 36)			✓	✓	2		obiekt mostowy
5.	Ścinawa - Most kolejowy (LK273)				✓	2		obiekt mostowy
6.	Brzeg Dolny - teren stopnia wodnego Brzeg Dolny, śluza Brzeg Dolny	✓	✓		✓	1	1	wieża
7.	Wrocław Rędzin - teren stopnia wodnego Rędzin, śluza Rędzin	✓	✓		✓		1	wieża
8.	Wrocław Osobowice - Most Milenijny (DK 5)			✓	✓	2		obiekt mostowy
9.	Wrocław Osobowice - Most kolejowy (LK 271)				✓	2		obiekt mostowy
10.	Wrocław Piasek - Most Pokoju				✓	2		obiekt mostowy
11.	Wrocław Piasek - Most Grunwaldzki (DW 372)			✓	✓	2		obiekt mostowy
12.	Wrocław Szczytniki - teren śluzy Szczytniki	✓	✓		✓	1	1	wieża
13.	Wrocław Dąbie - Kładka Zwierzyniecka				✓	2		obiekt mostowy
14.	Wrocław Dąbie - Most Olimpijski				✓	2		obiekt mostowy
15.	Wrocław Bartoszowice – teren stopnia wodnego Bartoszowice, śluza Bartoszowice	✓	✓		✓	1	1	wieża
16.	Brzeg – teren stopnia wodnego Brzeg	✓	✓		✓	1	1	wieża
17.	Opole Północ - Most Pamięci Sybiraków (DW 435)			✓	✓	2		obiekt mostowy
18.	Opole Centrum - Most kolejowy (LK 132)				✓	2		obiekt mostowy
19.	Opole Południe - Most im. Ireny Sendlerowej				✓	1		obiekt mostowy

Lp.	Lokalizacja	Funkcje				Kamery stałe	Kamery PTZ	Rodzaj obiektu
		R	M	H	O			
20.	Opole - teren nieczynnej stoczni rzecznej na wyspie Pasieka, teren PGW Wody Polskie – Nadzór Wodny Opole, ul. Jana Kochanowskiego 9.	✓	✓		✓	1	1	wieża
21.	Krapkowice - Most drogowy (DW 409) w ciągu ul. Księdza Koziołka			✓	✓	2		obiekt mostowy
22.	Kłodnica Północ - Most drogowy (DW 423) w ciągu ulicy Kłodnickiej			✓	✓	2		obiekt mostowy
23.	Koźle Południe - Most drogowy Józefa Długosza			✓	✓	2		obiekt mostowy
24.	Koźle Południe Ostrówek - teren obiektu Hydrotechnicznego Jaz Koźle, ul. Wyspa 20, 47-200 Kędzierzyn-Koźle, identyfikator działki: 160301_1.0014.2477/15 znajdującej się w pobliżu lądowiska przyszpitalnego H328.	✓	✓		✓	1	1	wieża

UWAGA:

Powyższe zestawienie nie obejmuje trzech istniejących lokalizacji na aktualnym obszarze funkcjonowania systemu RIS w których w ramach projektu „Rozbudowa systemu RIS na Odrzańskiej Drodze Wodnej” zostanie dodania funkcja obserwacyjna, tj.:

- Siekierki – Kładka pieszo-rowerowa na Odrze,
- Kostrzyn nad Odrą - Most kolejowy nr 2 na Warcie (Linia nr 273),
- Kostrzyn nad Odrą - Most drogowy na Warcie (DK 31).

Wskazane w tabeli funkcje lokalizacji, liczby urządzeń oraz rodzaje obiektów należy traktować jako minimalny zakres funkcjonalny i lokalizacyjny wynikający z PFU oraz dokumentów branżowych. Na etapie opracowania dokumentacji projektowej Generalny Wykonawca zobowiązany jest zweryfikować możliwość realizacji każdej lokalizacji, w tym warunki formalnoprawne, własnościowe, konstrukcyjne, środowiskowe, energetyczne, transmisyjne, montażowe i eksploatacyjne. Ostateczne rozwiązania lokalizacyjne, konstrukcyjne, instalacyjne i urządzeniowe wymagają uzgodnienia oraz akceptacji Zamawiającego, a w przypadkach wymaganych również właściwego właściciela, zarządcy nieruchomości, zarządcy obiektu lub właściwego organu administracji.

1.1.2. Opis rozbudowy i modernizacji systemu RIS

Rozdział przedstawia opis zasadniczych obszarów rozbudowy i modernizacji systemu RIS objętych przedmiotem zamówienia. Opis ma charakter ogólny i służy wskazaniu zakresu rzeczowego, skali oraz wzajemnych powiązań pomiędzy poszczególnymi częściami przedsięwzięcia, które łącznie mają doprowadzić do utworzenia spójnego, zintegrowanego i gotowego do eksploatacji zmodernizowanego systemu RIS na Odrzańskiej Drodze Wodnej.

Zakres opisany w niniejszym rozdziale obejmuje zarówno rozbudowę infrastruktury terenowej systemu RIS, w tym systemu łączności radiowej VHF/AIS/DGNSS, monitoringu wizyjnego CCTV, czujników hydrologicznych, sensorów meteorologicznych, sieci transmisji danych, wież, masztów, konstrukcji wsporczych i infrastruktury teletechnicznej, jak również modernizację i rozbudowę zaplecza technicznego oraz teleinformatycznego Zamawiającego. Obejmuje to w szczególności doposażenie serwerowni głównej, modernizację pomieszczenia serwerowni pełniącej rolę węzła telekomunikacyjnego, modernizację sieci teleinformatycznej, utworzenie środowiska pracy zmodernizowanego systemu RIS, utworzenie serwerowni zapasowej wraz z łączem teleinformatycznym, realizację usług cyfrowych RIS oraz objęcie zasobów infrastrukturalnych i aplikacyjnych monitoringiem technicznym.

Poszczególne elementy opisane w kolejnych podrozdziałach nie stanowią odrębnych, niezależnych zadań technicznych, lecz wzajemnie powiązane części jednego przedsięwzięcia. Generalny Wykonawca zobowiązany jest zaprojektować i wykonać je w sposób zapewniający spójność funkcjonalną, techniczną, transmisyjną, organizacyjną, bezpieczeństwa, utrzymaniową oraz eksploatacyjną całego systemu RIS. W szczególności urządzenia terenowe, konstrukcje wsporcze, zasilanie, transmisja danych, środowisko serwerowe, usługi cyfrowe, integracje, monitoring techniczny oraz zaplecze operatorskie i administracyjne muszą tworzyć jednolite środowisko świadczenia usług informacji rzecznej.

Opisy zamieszczone w niniejszym rozdziale określają ogólny zakres przedmiotu zamówienia dla poszczególnych obszarów realizacji. Szczegółowe wymagania Zamawiającego dotyczące projektowania, dostaw, robót, instalacji, konfiguracji, integracji, testów, odbiorów, dokumentacji, gwarancji, serwisu, cyberbezpieczeństwa, interoperacyjności i utrzymania zostały określone w rozdziale 1.2 PFU oraz w dokumentach branżowych stanowiących załączniki do PFU, w szczególności w Planie systemu monitoringu wizyjnego, Planie łączności radiowej VHF/AIS oraz Planie połączeń transmisyjnych.

1.1.2.1. Rozbudowa systemu łączności radiowej VHF/AIS/DGNSS

Przedmiot zamówienia obejmuje rozbudowę systemu łączności radiowej VHF/AIS/DGNSS stanowiącego jeden z podstawowych podsystemów infrastruktury RIS na Odrzańskiej Drodze Wodnej. Zakres ten obejmuje zaprojektowanie, dostawę, montaż, konfigurację, uruchomienie, integrację, przetestowanie i przekazanie do eksploatacji nowych oraz jeżeli wynika to z przyjętego rozwiązania, modernizowanych elementów podsystemu radiowego RIS.

Punktem wyjścia dla projektowanej rozbudowy jest funkcjonujący obecnie podsystem łączności radiowej RIS Dolnej Odry. W stanie istniejącym warstwa AIS obejmuje 8 lokalizacji, warstwa VHF obejmuje 7 lokalizacji, a 7 lokalizacji pełni równocześnie funkcje AIS i VHF. Istniejąca warstwa

AIS wykorzystuje stacje brzegowe AIS pracujące w układzie podstawowym i zapasowym, natomiast istniejąca warstwa VHF obejmuje 14 kompletów stacji brzegowych VHF, system dyspozytorski pracujący w układzie pary niezawodnościowej, rejestrator głosu i danych powiązanych, serwer API oraz 4 komplety konsol dyspozytorskich VHF. Rozbudowa systemu musi uwzględniać ten stan jako punkt odniesienia dla zapewnienia spójności architektury, ciągłości działania, kompatybilności i integracji nowych elementów z istniejącym systemem RIS.

W ramach rozbudowy przewiduje się realizację 8 nowych lokalizacji obiektów AIS i VHF, obejmujących lokalizacje wskazane w dokumencie branżowym jako AIS 1 – AIS 8 oraz VHF 1 – VHF 8. Lokalizacje te obejmują zasadniczy obszar rozbudowy systemu RIS na Odrzańskiej Drodze Wodnej, w tym w szczególności odcinek od rejonu Ścinawy, przez Brzeg Dolny, Wrocławski Węzeł Wodny, Brzeg i Opole, do rejonu Kędzierzyna-Koźla.

Zakres projektowanej rozbudowy obejmuje w szczególności realizację nowych stacji brzegowych AIS, nowych stacji brzegowych VHF, funkcji dystrybucji poprawek DGNSS, systemów antenowych, torów antenowych, urządzeń radiokomunikacyjnych, urządzeń sterowania, urządzeń nadzoru technicznego, urządzeń zasilania podstawowego i rezerwowego, elementów transmisji danych, szaf teletechnicznych, konstrukcji wsporczych, instalacji uziemiających, ochrony odgromowej, ochrony przepięciowej oraz wyposażenia pomocniczego niezbędnego do całorocznej eksploatacji podsystemu.

W odniesieniu do warstwy AIS przewiduje się, że każda nowa lokalizacja AIS zostanie wyposażona w układ pracy podstawowej i zapasowej, zapewniający utrzymanie funkcji AIS w przypadku awarii pojedynczego urządzenia bazowego. Oznacza to konieczność dostarczenia i uruchomienia w każdej lokalizacji AIS dwóch stacji brzegowych AIS klasy A albo rozwiązania równoważnego funkcjonalnie, zapewniającego pracę podstawową i zapasową oraz obsługę kanałów AIS1/AIS A i AIS2/AIS B zgodnie z warunkami właściwego pozwolenia radiowego.

W odniesieniu do warstwy VHF przewiduje się realizację stacji bazowych VHF w lokalizacjach przeznaczonych dla łączności głosowej. System ma zapewniać prowadzenie łączności głosowej pomiędzy uprawnionymi użytkownikami systemu RIS a jednostkami pływającymi znajdującymi się w obszarze pokrycia radiowego danej stacji. Rozwiązanie musi umożliwiać centralną obsługę, zdalne sterowanie, nadzór techniczny, rejestrację zdarzeń oraz integrację z operatorskim środowiskiem łączności radiowej RIS.

Rozbudowa podsystemu ma zapewnić rozszerzenie zasięgu i funkcjonalności usług RIS na obszarze objętym projektem, w szczególności w zakresie automatycznej identyfikacji jednostek pływających AIS, dystrybucji poprawek DGNSS, łączności głosowej VHF, centralnej obsługi operatorskiej, nadzoru technicznego, rejestracji zdarzeń oraz integracji z pozostałymi komponentami systemu RIS.

Zakres rzeczowy tej części zamówienia obejmuje w szczególności:

1) realizację 8 nowych lokalizacji stacji brzegowych AIS i VHF wskazanych w dokumencie branżowym jako AIS 1–AIS 8 oraz VHF 1–VHF 8;
2) dostawę i uruchomienie stacji brzegowych AIS w układzie podstawowym i zapasowym dla każdej lokalizacji AIS;
3) dostawę i uruchomienie stacji brzegowych VHF dla lokalizacji przewidzianych dla warstwy łączności głosowej;

4) zapewnienie funkcji dystrybucji poprawek DGNSS w zakresie wymaganym dla systemu RIS;
5) zaprojektowanie i wykonanie systemów antenowych, torów antenowych, okablowania, zabezpieczeń, zasilania, transmisji danych i elementów montażowych;
6) dostawę i uruchomienie urządzeń radiokomunikacyjnych, urządzeń sterowania, urządzeń nadzoru technicznego oraz wyposażenia pomocniczego;
7) zapewnienie integracji nowych komponentów z systemami centralnymi RIS, środowiskiem operatorskim, systemami nadzoru, rejestracji, alarmowania i diagnostyki;
8) zapewnienie komunikacji pomiędzy lokalizacjami terenowymi a Centrum RIS zgodnie z wymaganiami dotyczącymi transmisji danych;
9) opracowanie dokumentacji projektowej, wykonawczej, powykonawczej, konfiguracyjnej, odbiorowej i eksploatacyjnej;
10) uzyskanie albo przygotowanie dokumentacji niezbędnej do uzyskania wymaganych pozwoleń radiowych, zgód, uzgodnień i decyzji administracyjnych;
11) przeprowadzenie testów funkcjonalnych, technicznych, zasięgowych, integracyjnych i odbiorowych.

System łączności radiowej VHF/AIS/DGNSS musi zostać zaprojektowany i wykonany jako element jednego, spójnego systemu RIS. Oznacza to, że nowe i modernizowane komponenty muszą współpracować z istniejącą architekturą systemu RIS, nie mogą pogarszać pracy dotychczasowych komponentów oraz muszą zapewniać możliwość centralnego nadzoru, obsługi operatorskiej, rejestracji zdarzeń, diagnostyki i utrzymania.

Generalny Wykonawca zobowiązany jest traktować lokalizacje, konfiguracje, analizy propagacyjne, rekomendacje techniczno-instalacyjne oraz wymagania zawarte w PFU i w dokumencie „PLAN ŁĄCZNOŚCI RADIOWEJ VHF/AIS” jako materiał wejściowy do projektowania. Na etapie opracowania dokumentacji projektowej Generalny Wykonawca ma obowiązek zweryfikować aktualność założeń terenowych, formalnych, technicznych, propagacyjnych, instalacyjnych i eksploatacyjnych oraz potwierdzić możliwość realizacji rozwiązania w każdej lokalizacji.

Realizacja nowych lokalizacji VHF/AIS/DGNSS będzie powiązana z wykonaniem obiektów wieżowych stacji radiokomunikacyjnych oraz infrastruktury terenowej niezbędnej do pracy urządzeń radiowych i transmisyjnych. Obiekty wieżowe będą stanowiły platformę dla systemów antenowych, torów antenowych oraz innych elementów wymagających wyniesienia na wysokość, natomiast urządzenia stacji brzegowych VHF/AIS/DGNSS oraz urządzenia towarzyszące będą lokalizowane w odpowiedniej infrastrukturze technicznej, w szczególności w szafach teletechnicznych typu zewnętrznego. Szczegółowe wymagania dotyczące obiektów wieżowych, szaf teletechnicznych, instalacji antenowych, zasilania, transmisji danych, ochrony odgromowej, uziemienia, ochrony przepięciowej, montażu i odbiorów zostały określone w dalszej części PFU oraz w dokumencie „PLAN ŁĄCZNOŚCI RADIOWEJ VHF/AIS”.

Szczegółowy zakres lokalizacji, liczba i konfiguracja urządzeń, wymagania techniczne, wymagania funkcjonalne, wyniki analiz propagacyjnych, wymagania dotyczące stacji AIS, stacji VHF, dystrybucji poprawek DGNSS, konsol operatorskich, integracji, pozwoleń radiowych, instalacji antenowych, zasilania, transmisji danych, nadzoru technicznego, testów i odbiorów określa dokument „PLAN ŁĄCZNOŚCI RADIOWEJ VHF/AIS”, stanowiący dokument branżowy PFU.

1.1.2.2. Rozbudowa i modernizacja systemu monitoringu wizyjnego (CCTV)

Przedmiot zamówienia obejmuje rozbudowę i modernizację systemu monitoringu wizyjnego CCTV stanowiącego jeden z podsystemów infrastruktury RIS na Odrzańskiej Drodze Wodnej. Zakres ten obejmuje zaprojektowanie, dostawę, montaż, konfigurację, uruchomienie, integrację, przetestowanie i przekazanie do eksploatacji nowych oraz modernizowanych elementów systemu CCTV.

System CCTV funkcjonujący obecnie w ramach RIS Dolnej Odry obejmuje łącznie 53 kamery rozmieszczone w 30 lokalizacjach, w tym 48 kamer stałych oraz 5 kamer obrotowych PTZ. Istniejący system opiera się na centralnej rejestracji obrazu w Centrum RIS, wykorzystuje rejestratory NVR, ścianę wizyjną, stanowiska operatorskie oraz mechanizmy udostępniania obrazu w ramach aplikacji systemu RIS. Rozbudowa i modernizacja systemu CCTV musi uwzględniać ten stan jako punkt wyjścia dla zaprojektowania docelowego rozwiązania, przy zachowaniu ciągłości funkcji operacyjnych i bez pogorszenia zakresu funkcjonalnego obecnie dostępnego dla Zamawiającego.

W ramach rozbudowy i modernizacji podsystemu CCTV przewiduje się w szczególności dostawę i uruchomienie 50 nowych kamer obserwacyjnych, w tym 41 kamer stałych oraz 9 kamer PTZ, przeznaczonych do obserwacji drogi wodnej, obiektów mostowych, obiektów hydrotechnicznych oraz lokalizacji istotnych z punktu widzenia funkcji RIS. Zakres obejmuje również dostawę i uruchomienie 16 nowych kamer dozorowych przeznaczonych do nadzoru wież radiowych, szaf teletechnicznych typu zewnętrznego oraz infrastruktury terenowej.

Zakres rzeczowy obejmuje ponadto budowę lub modernizację warstwy centralnej systemu CCTV, w tym zapewnienie nowej platformy rejestracji źródeł obrazu obserwacyjnego pracującej w układzie wysokiej dostępności, obejmującej 2 węzły/rejestratory. Platforma ta ma umożliwiać obsługę 103 kanałów z kamer własnych systemu RIS oraz 18 strumieni wideo udostępnianych przez Krajowy Zarząd Gospodarki Wodnej PGW Wody Polskie, z zachowaniem rezerwy rozwojowej. Zakres obejmuje również dostawę 3 kompletów stacji klienckich systemu CCTV wraz z wyposażeniem prezentacyjnym.

Rozbudowa systemu CCTV obejmuje zarówno nowe punkty obserwacyjne, modernizację wybranych istniejących punktów obserwacyjnych, wykorzystanie strumieni wideo udostępnianych przez PGW Wody Polskie, jak również punkty dozorowe infrastruktury technicznej RIS. W szczególności system ma objąć nowe lokalizacje kamerowe na obszarze planowanej rozbudowy RIS na Odrzańskiej Drodze Wodnej, lokalizacje punktowe na obszarze obecnie działającego systemu RIS Dolnej Odry oraz lokalizacje związane z dozorem infrastruktury radiokomunikacyjnej i teletechnicznej.

System monitoringu wizyjnego CCTV ma wspierać realizację usług RIS poprzez zapewnienie obserwacji miejsc istotnych z punktu widzenia bezpieczeństwa ruchu żeglugowego, nadzoru nad drogą wodną, nadzoru nad wybranymi obiektami infrastruktury technicznej, oceny warunków nawigacyjnych oraz wsparcia pracy operatorów Centrum RIS i innych uprawnionych użytkowników systemu.

Zakres rzeczowy tej części zamówienia obejmuje w szczególności:

1) realizację nowych punktów obserwacyjnych systemu CCTV;
2) modernizację wybranych istniejących punktów obserwacyjnych systemu CCTV, jeżeli wynika to z przyjętego rozwiązania projektowego;
3) dostawę, montaż i konfigurację nowych kamer obserwacyjnych, kamer dozorowych, kamer PTZ oraz wyposażenia pomocniczego;
4) wykonanie instalacji kablowych, zasilających, transmisyjnych, montażowych, ochronnych i uziemiających niezbędnych do pracy punktów kamerowych;
5) zapewnienie transmisji strumieni wideo z lokalizacji terenowych do warstwy centralnej systemu;
6) zapewnienie rejestracji, archiwizacji, odtwarzania i eksportu nagrań;
7) dostawę, rozbudowę lub konfigurację platformy rejestracji i obsługi obrazu;
8) dostawę lub modernizację stanowisk operatorskich, stacji klienckich, środowiska prezentacji obrazu oraz narzędzi obsługi systemu;
9) zapewnienie integracji systemu CCTV z pozostałymi komponentami RIS;
10) zapewnienie mechanizmów ochrony prywatności, kontroli uprawnień, monitoringu technicznego, alarmowania i utrzymania;
11) opracowanie dokumentacji projektowej, wykonawczej, powykonawczej, konfiguracyjnej, odbiorowej i eksploatacyjnej;
12) przeprowadzenie testów technicznych, funkcjonalnych, integracyjnych, bezpieczeństwa, odpornościowych i odbiorowych.

System CCTV musi zostać zaprojektowany i wykonany jako element zintegrowanego systemu RIS, a nie jako odrębny, autonomiczny system dozoru wizyjnego. Oznacza to, że projektowane rozwiązanie musi zapewniać możliwość współpracy z systemem RIS, systemami operatorskimi, narzędziami prezentacji obrazu, mechanizmami zarządzania uprawnieniami, systemami monitoringu technicznego, systemem transmisji danych oraz innymi komponentami objętymi przedmiotem zamówienia.

Rozbudowa i modernizacja systemu CCTV obejmuje zarówno warstwę terenową, jak i warstwę centralną. Warstwa terenowa obejmuje punkty kamerowe, kamery, konstrukcje montażowe, szafy, zasilanie, transmisję danych, zabezpieczenia, okablowanie i elementy instalacyjne. Warstwa centralna obejmuje platformę rejestracji, archiwizacji i udostępniania obrazu, stanowiska operatorskie, środowisko prezentacji obrazu, narzędzia administracyjne, narzędzia eksportu materiału, mechanizmy monitoringu technicznego oraz integrację z pozostałymi systemami.

Generalny Wykonawca zobowiązany jest traktować lokalizacje, kierunki obserwacji, widoki referencyjne, wymagania transmisyjne, wymagania retencji, wymagania integracyjne oraz pozostałe założenia zawarte w PFU i w dokumencie „PLAN SYSTEMU MONITORINGU WIZYJNEGO (CCTV)” jako materiał wejściowy do projektowania. Na etapie opracowania dokumentacji projektowej Generalny Wykonawca ma obowiązek zweryfikować aktualność założeń terenowych, formalnych, technicznych, montażowych, transmisyjnych, funkcjonalnych i eksploatacyjnych oraz potwierdzić możliwość realizacji rozwiązania w każdej lokalizacji.

Realizacja punktów obserwacyjnych i dozorowych CCTV będzie powiązana z wykorzystaniem odpowiedniej infrastruktury nośnej i terenowej, dostosowanej do funkcji danego punktu kamerowego oraz warunków lokalizacyjnych. Platformą nośną dla kamer obserwacyjnych i dozorowych będą w szczególności obiekty mostowe, obiekty wieżowe, słupy kamerowe oraz inne konstrukcje wsporcze dostosowane do specyfiki lokalizacji i zaakceptowane w dokumentacji projektowej. Urządzenia towarzyszące systemu CCTV, w tym urządzenia transmisji danych, zasilania, sterowania, zabezpieczeń i monitoringu technicznego, będą lokalizowane w odpowiedniej infrastrukturze technicznej, w szczególności w szafach teletechnicznych typu zewnętrznego. Szczegółowe wymagania dotyczące projektowania punktów kamerowych, konstrukcji wsporczych, szaf teletechnicznych, instalacji kablowych, zasilania, transmisji danych, zabezpieczeń, montażu, ochrony prywatności, testów i odbiorów zostały określone w dalszej części PFU oraz w dokumencie „PLAN SYSTEMU MONITORINGU WIZYJNEGO (CCTV)”.

Szczegółowy zakres lokalizacji, liczby i typy urządzeń, wymagania techniczne, wymagania funkcjonalne, wymagania dotyczące kamer, platformy rejestracji, stacji klienckich, transmisji strumieni wideo, retencji, integracji, bezpieczeństwa, ochrony prywatności, monitoringu technicznego, instalacji kablowych, instalacji montażowych, narzędzi obsługi, testów i odbiorów określa dokument „PLAN SYSTEMU MONITORINGU WIZYJNEGO (CCTV)”, stanowiący dokument branżowy PFU.

1.1.2.3. Rozbudowa sieci transmisji danych

Przedmiot zamówienia obejmuje rozbudowę sieci transmisji danych systemu RIS na Odrzańskiej Drodze Wodnej, stanowiącej warstwę komunikacyjną dla nowych i modernizowanych komponentów systemu RIS. Sieć transmisji danych musi zapewniać wymianę danych cyfrowych, strumieni wideo, danych telemetrycznych, sygnałów sterowania, informacji diagnostycznych i alarmów pomiędzy lokalizacjami terenowymi, Centrum RIS, serwerownią główną, serwerownią zapasową, systemami centralnymi oraz pozostałymi komponentami objętymi przedmiotem zamówienia.

Punktem wyjścia dla projektowanej rozbudowy jest istniejąca sieć transmisji danych RIS Dolnej Odry. W stanie istniejącym sieć obejmuje łącznie 77 opisanych łącz transmisyjnych, w tym 39 relacji podstawowych oraz 38 relacji zapasowych i dodatkowych. Istniejąca sieć ma charakter hybrydowy i wykorzystuje w szczególności radiolinie punkt–punkt w paśmie nielicencjonowanym, lokalne połączenia przewodowe i optotelekomunikacyjne, łącza LTE, połączenia operatorskie oraz mechanizmy VPN i przełączenia awaryjnego. Rozbudowa sieci transmisji danych musi uwzględniać ten stan jako punkt odniesienia dla zapewnienia spójności architektury,

kompatybilności, bezpieczeństwa, ciągłości działania i integracji nowych elementów z istniejącym środowiskiem RIS.

W ramach rozbudowy systemu RIS przewiduje się zapewnienie transmisji danych dla nowych lokalizacji terenowych oraz dla lokalizacji modernizowanych, w których zostaną zainstalowane lub wykorzystane komponenty systemu RIS, w szczególności stacje VHF/AIS/DGNSS, kamery CCTV, czujniki hydrologiczne, czujniki meteorologiczne, urządzenia nadzoru technicznego, urządzenia zasilania i urządzenia bezpieczeństwa. Dokument branżowy identyfikuje 22 lokalizacje terenowe analizowane pod kątem zastosowania redundantnych torów dostępowych oraz 24 potencjalne relacje radioliniowe, które zostały poddane analizie możliwości realizacji w paśmie nielicencjonowanym.

Zakres projektowanej rozbudowy obejmuje w szczególności zaprojektowanie, dostawę, montaż, konfigurację, uruchomienie, integrację, testowanie i przekazanie do eksploatacji urządzeń, usług, łączy, konfiguracji i mechanizmów niezbędnych do zapewnienia komunikacji pomiędzy lokalizacjami terenowymi a Centrum RIS. Generalny Wykonawca zobowiązany jest zapewnić transmisję danych dla każdego punktu objętego zakresem zamówienia w sposób dostosowany do rodzaju urządzeń, przewidywanego wolumenu ruchu, wymagań przepustowościowych, wymagań dostępnościowych, wymagań bezpieczeństwa i wymagań eksploatacyjnych.

Zakres rzeczowy tej części zamówienia obejmuje w szczególności:

1) zaprojektowanie docelowej architektury sieci transmisji danych dla nowych lokalizacji systemu RIS oraz dla istniejących elementów sieci transmisyjnej, których wykorzystanie, rozbudowa lub rekonfiguracja będzie niezbędna do włączenia nowych komponentów do systemu RIS;
2) zapewnienie komunikacji pomiędzy lokalizacjami terenowymi a Centrum RIS, serwerownią główną, serwerownią zapasową oraz pozostałymi środowiskami systemowymi;
3) zapewnienie transmisji danych dla stacji VHF/AIS/DGNSS, kamer CCTV, czujników hydrologicznych i meteorologicznych, urządzeń monitoringu technicznego, urządzeń zasilania oraz innych komponentów systemu RIS;
4) zaprojektowanie i uruchomienie torów podstawowych oraz torów zapasowych transmisji danych dla lokalizacji objętych zakresem zamówienia;
5) wykorzystanie technologii transmisyjnych właściwych dla danej lokalizacji, w tym łączy operatorskich, łączy komórkowych, łączy przewodowych, światłowodowych, radioliniowych albo innych rozwiązań zaakceptowanych przez Zamawiającego;
6) dostawę, montaż i konfigurację urządzeń brzegowych, routerów, modemów, anten, przełączników, urządzeń bezpieczeństwa, urządzeń monitoringu oraz wyposażenia pomocniczego;
7) zapewnienie segmentacji sieci, adresacji IP, nazewnictwa urządzeń, reguł dostępu, szyfrowania transmisji, tuneli VPN, mechanizmów routingu i mechanizmów przełączania awaryjnego;
8) zapewnienie monitoringu, diagnostyki, alarmowania i zdalnego utrzymania urządzeń oraz łączy transmisyjnych;

9) zapewnienie integracji nowych połączeń transmisyjnych z istniejącą siecią RIS oraz z docelowymi narzędziami administracyjnymi, monitorującymi i utrzymaniowymi;
10) opracowanie dokumentacji projektowej, wykonawczej, powykonawczej, konfiguracyjnej, odbiorowej i eksploatacyjnej dla sieci transmisji danych;
11) przeprowadzenie testów funkcjonalnych, technicznych, przepustowościowych, bezpieczeństwa, przełączenia awaryjnego, monitoringu, integracji i odbioru.

Docelowa sieć transmisji danych musi zostać zaprojektowana jako jeden spójny podsystem transmisyjny systemu RIS, a nie jako zbiór niezależnych, lokalnych rozwiązań komunikacyjnych. Oznacza to, że nowe i modernizowane łącza, urządzenia i konfiguracje muszą być zgodne z architekturą logiczną systemu RIS, planem adresacji, zasadami segmentacji, zasadami bezpieczeństwa, modelem monitorowania, zasadami wykonywania kopii konfiguracji oraz wymaganiami eksploatacyjnymi Zamawiającego.

Generalny Wykonawca zobowiązany jest traktować założenia, wykazy lokalizacji, analizy radioliniowe, analizy dostępności łączy operatorskich, karty lokalizacyjne BTS, wymagania przepustowościowe oraz pozostałe informacje zawarte w PFU i w dokumencie „PLAN POŁĄCZEŃ TRANSMISYJNYCH” jako materiał wejściowy do projektowania. Na etapie opracowania dokumentacji projektowej Generalny Wykonawca ma obowiązek zweryfikować aktualność założeń terenowych, technicznych, operatorskich, formalnych, transmisyjnych i eksploatacyjnych oraz potwierdzić możliwość realizacji przyjętego rozwiązania dla każdej lokalizacji.

Realizacja połączeń transmisyjnych w lokalizacjach terenowych będzie powiązana z wykorzystaniem odpowiedniej infrastruktury nośnej i teletechnicznej, dostosowanej do funkcji danego punktu oraz warunków lokalizacyjnych. Platformą nośną dla anten transmisyjnych, torów antenowych oraz innych elementów wymagających wyniesienia na wysokość będą w szczególności obiekty mostowe, obiekty wieżowe, słupy kamerowe oraz inne konstrukcje wsporcze dostosowane do specyfiki lokalizacji i zaakceptowane w dokumentacji projektowej. Urządzenia aktywne sieci transmisji danych oraz urządzenia towarzyszące, w tym, przełączniki, urządzenia zasilania, zabezpieczeń, sterowania i monitoringu technicznego, będą lokalizowane w odpowiedniej infrastrukturze technicznej, w szczególności w szafach teletechnicznych typu zewnętrznego. Szczegółowe wymagania dotyczące projektowania połączeń transmisyjnych, urządzeń aktywnych, anten, torów antenowych, szaf teletechnicznych, zasilania, transmisji danych, zabezpieczeń, monitoringu, diagnostyki, testów i odbiorów zostały określone w dalszej części PFU oraz w dokumencie „PLAN POŁĄCZEŃ TRANSMISYJNYCH”.

Szczegółowy zakres lokalizacji, relacji transmisyjnych, wymagania przepustowościowe, wymagania funkcjonalne, wymagania bezpieczeństwa, zasady redundancji, wyniki analiz radioliniowych, wyniki analiz dostępności łączy operatorskich, zasady doboru torów podstawowych i zapasowych, schemat sieci transmisyjnej, wymagania dotyczące monitoringu, diagnostyki, dokumentacji, testów i odbiorów określa dokument „PLAN POŁĄCZEŃ TRANSMISYJNYCH”, stanowiący dokument branżowy PFU.

1.1.2.4. Czujniki hydrologiczne (wodowskazy)

Przedmiot zamówienia obejmuje zaprojektowanie, dostawę, montaż, konfigurację, uruchomienie, integrację, przetestowanie i przekazanie do eksploatacji czujników hydrologicznych, pełniących funkcję wodowskazów systemu RIS na Odrzańskiej Drodze Wodnej. Czujniki hydrologiczne będą stanowiły źródło danych pomiarowych o stanie wody, wykorzystywanych przez system RIS, Centrum RIS, usługi cyfrowe, usługi informacji hydrometeorologicznej, aplikacje operatorskie oraz inne komponenty systemu RIS wskazane w PFU.

Zakres tej części zamówienia obejmuje realizację czujników hydrologicznych w 8 lokalizacjach mostowych:

1) Szczecin Podjuchy – Most kolejowy im. dr. inż. Andrzeja Krefta;
2) Ścinawa – Most drogowy DK 36;
3) Wrocław Osobowice – Most Milenijny DK 5;
4) Wrocław Piasek – Most Grunwaldzki DW 372;
5) Opole Północ – Most Pamięci Sybiraków DW 435;
6) Krapkowice – Most drogowy DW 409 w ciągu ul. Księdza Koziołka;
7) Kłodnica Północ – Most drogowy DW 423 w ciągu ul. Kłodnickiej;
8) Koźle Południe – Most drogowy Józefa Długosza.

W każdej lokalizacji należy przewidzieć redundantny układ pomiarowy obejmujący co najmniej dwa niezależne czujniki pomiarowe albo rozwiązanie równoważne funkcjonalnie, zapewniające możliwość weryfikacji poprawności wskazań, wykrywania rozbieżności pomiarowych oraz utrzymania funkcji pomiarowej w przypadku awarii pojedynczego toru pomiarowego. Oznacza to, że zakres zamówienia obejmuje co najmniej 16 torów pomiarowych w 8 lokalizacjach wodowskazowych.

Czujniki hydrologiczne będą instalowane na obiektach mostowych na konstrukcjach wsporczych dostosowanych do specyfiki danej lokalizacji, warunków pomiarowych, warunków montażowych oraz wymagań właściwego zarządcy obiektu. Urządzenia pomiarowe powinny być lokalizowane w sposób umożliwiający pomiar poziomu lustra wody bez ograniczania prześwitu pionowego i szerokości użytkowej przęseł żeglownych oraz bez negatywnego wpływu na funkcję i bezpieczeństwo obiektu mostowego.

Realizacja wodowskazów będzie powiązana z wykonaniem infrastruktury terenowej niezbędnej do pracy urządzeń pomiarowych, w szczególności konstrukcji montażowych, tras kablowych, zasilania, transmisji danych, zabezpieczeń, uziemienia, ochrony przepięciowej, urządzeń diagnostycznych, urządzeń komunikacyjnych oraz szaf teletechnicznych typu zewnętrznego albo innych obudów technicznych dostosowanych do pracy całorocznej w warunkach terenowych. Szczegółowe wymagania dla tej infrastruktury określają właściwe rozdziały PFU dotyczące konstrukcji wsporczych, szaf teletechnicznych, zasilania, transmisji danych, ochrony odgromowej, uziemienia, ochrony przepięciowej, dokumentacji i odbiorów.

Na odcinku Dolnej Odry Zamawiający eksploatuje sterowniki i wyświetlacze do czujników poziomu VEGAMET 624 oraz VEGAMET 625 wraz z sondami radarowymi do ciągłego pomiaru poziomu cieczy VEGAPULS 61. Informacja ta ma charakter opisu stanu istniejącego i punktu odniesienia dla zapewnienia ciągłości koncepcji pomiarowej, sposobu eksploatacji, integracji danych, utrzymania oraz dokumentacji systemu RIS. Nie oznacza ona ograniczenia konkurencji ani obowiązku zastosowania urządzeń wskazanego producenta, o ile Generalny Wykonawca zapewni rozwiązanie równoważne funkcjonalnie, technicznie i eksploatacyjnie, spełniające wymagania PFU.

Czujniki hydrologiczne mają zapewniać bieżące pozyskiwanie danych pomiarowych, ich lokalną obsługę, diagnostykę, transmisję do systemu RIS, kontrolę jakości pomiaru, możliwość konfiguracji parametrów pracy oraz wykorzystanie danych przez komponenty systemu RIS. Dane pomiarowe mają być przygotowane do wykorzystania w systemach informacji hydrometeorologicznej, usługach cyfrowych RIS, aplikacjach operatorskich, aplikacjach dla użytkowników śródlądowych dróg wodnych, komunikatach i prezentacjach dotyczących warunków nawigacyjnych oraz jeżeli zostanie to przewidziane w architekturze docelowej, do przekazywania właściwym interesariuszom zewnętrznym.

Punktem odniesienia dla ustalania wartości pomiarowych, kalibracji, weryfikacji i powiązania pomiaru z właściwym układem odniesienia ma być Operat Techniczny z pomiarów wodowskazów na obszarze działania rozbudowy systemu RIS na Odrzańskiej Drodze Wodnej, opracowany przez Generalnego Wykonawcę na potrzeby niniejszego zamówienia i zaakceptowany przez Zamawiającego.

Szczegółowe wymagania dotyczące lokalizacji, sposobu montażu, redundancji pomiaru, parametrów czujników, transmisji danych, kalibracji, odniesienia wysokościowego, diagnostyki, integracji z systemem RIS, tras kablowych, zasilania, dokumentacji, testów, odbiorów, gwarancji, serwisu i utrzymania określają dalsze rozdziały PFU, w szczególności rozdział 1.2.6 oraz rozdziały dotyczące infrastruktury teletechnicznej terenowej, transmisji danych, zasilania, dokumentacji, testów i przekazania do eksploatacji.

1.1.2.5. Sensory meteorologiczne

Przedmiot zamówienia obejmuje zaprojektowanie, dostawę, montaż, konfigurację, uruchomienie, integrację, przetestowanie i przekazanie do eksploatacji sensorów meteorologicznych stanowiących element segmentu źródeł danych systemu RIS na Odrzańskiej Drodze Wodnej. Sensory meteorologiczne będą służyły do pozyskiwania danych o bieżących warunkach atmosferycznych w lokalizacjach istotnych z punktu widzenia bezpieczeństwa żeglugi, pracy operatorów Centrum RIS, świadczenia usług informacji hydrometeorologicznej oraz prezentacji danych w aplikacjach i usługach cyfrowych systemu RIS.

Zakres tej części zamówienia obejmuje realizację sensorów meteorologicznych w 8 lokalizacjach terenowych:

1) Ścinawa;
2) Brzeg Dolny – teren stopnia wodnego Brzeg Dolny, śluza Brzeg Dolny;
3) Wrocław Rędzin – teren stopnia wodnego Rędzin, śluza Rędzin;

4) Wrocław Szczytniki – teren śluzy Szczytniki, Wyspa Szczytniki;
5) Wrocław Bartoszowice – teren stopnia wodnego Bartoszowice, śluza Bartoszowice;
6) Brzeg – teren stopnia wodnego Brzeg;
7) Opole – teren nieczynnej stoczni rzecznej na wyspie Pasieka, teren PGW Wody Polskie – Nadzór Wodny Opole, ul. Jana Kochanowskiego 9;
8) Koźle Południe Ostrówek – teren obiektu hydrotechnicznego Jaz Koźle, ul. Wyspa 20, 47-200 Kędzierzyn-Koźle.

W każdej lokalizacji należy przewidzieć co najmniej jeden kompletny sensor meteorologiczny albo zespół sensorów meteorologicznych zapewniających pomiar, rejestrację i transmisję danych dotyczących podstawowych parametrów atmosferycznych. Oznacza to, że zakres zamówienia obejmuje co najmniej 8 punktów pomiaru meteorologicznego wraz z infrastrukturą montażową, zasilającą, transmisyjną, zabezpieczającą i integracyjną niezbędną do ich pracy w systemie RIS.

Sensory meteorologiczne mają zapewniać co najmniej pomiar prędkości i kierunku wiatru, opadów atmosferycznych, ciśnienia barometrycznego, temperatury powietrza oraz wilgotności względnej. Jeżeli zastosowane rozwiązanie techniczne umożliwia pomiar dodatkowych parametrów, takich jak intensywność zjawisk gradowych, czas trwania opadu, intensywność opadu lub inne parametry środowiskowe, dane te powinny zostać udostępnione w systemie RIS, o ile ich wykorzystanie zostanie przewidziane w dokumentacji projektowej i zaakceptowane przez Zamawiającego.

Na odcinku Dolnej Odry Zamawiający eksploatuje czujniki meteorologiczne Vaisala WXT536. Informacja ta ma charakter opisu stanu istniejącego i punktu odniesienia dla zachowania ciągłości koncepcji pomiarowej, integracji danych, sposobu eksploatacji, diagnostyki, dokumentacji i utrzymania systemu RIS. Nie oznacza ona ograniczenia konkurencji ani obowiązku zastosowania urządzeń wskazanego producenta, o ile Generalny Wykonawca zapewni rozwiązanie równoważne funkcjonalnie, technicznie i eksploatacyjnie, spełniające wymagania PFU.

Sensory meteorologiczne będą powiązane z infrastrukturą terenową nowych lokalizacji RIS, w szczególności z obiektami wieżowymi stacji radiokomunikacyjnych VHF/AIS/DGNSS, siecią transmisji danych, zasilaniem, monitoringiem technicznym, szafami teletechnicznymi typu zewnętrznego oraz systemami centralnymi RIS. Platformą montażową sensorów meteorologicznych będą obiekty oraz konstrukcje wsporcze zaakceptowane w dokumentacji projektowej, o ile zapewnią spełnienie wymagań pomiarowych, instalacyjnych, eksploatacyjnych i bezpieczeństwa.

Sensory meteorologiczne mają lokalizowane w sposób umożliwiający pozyskiwanie reprezentatywnych danych o warunkach atmosferycznych w danej lokalizacji. W szczególności należy unikać montażu w miejscach przesłoniętych przez drzewa, budynki, konstrukcje, ekrany, elementy infrastruktury technicznej albo inne obiekty mogące zniekształcać pomiar prędkości i kierunku wiatru, opadu, temperatury, wilgotności lub ciśnienia.

Realizacja sensorów meteorologicznych będzie obejmowała również wykonanie albo wykorzystanie infrastruktury terenowej niezbędnej do ich pracy, w szczególności konstrukcji

montażowych, tras kablowych, przewodów sygnałowych, przewodów zasilających, elementów transmisji danych, zabezpieczeń, ochrony przepięciowej, uziemienia, urządzeń diagnostycznych oraz elementów umożliwiających bezpieczny dostęp serwisowy. Szczegółowe wymagania dla tej infrastruktury określają właściwe rozdziały PFU dotyczące obiektów wieżowych, konstrukcji wsporczych, szaf teletechnicznych, zasilania, transmisji danych, ochrony odgromowej, uziemienia, ochrony przepięciowej, dokumentacji i odbiorów.

Dane meteorologiczne mają być przekazywane do systemu RIS w sposób umożliwiający ich bieżące wykorzystanie przez Centrum RIS, aplikacje operatorskie, usługi cyfrowe RIS, usługę informacji hydrometeorologicznej, aplikację mapową dla użytkowników śródlądowych dróg wodnych oraz inne komponenty systemu wskazane w dokumentacji projektowej. Dane te powinny wspierać ocenę warunków nawigacyjnych, analizę sytuacji na drodze wodnej, informowanie użytkowników Odrzańskiej Drogi Wodnej oraz budowę spójnego obrazu sytuacyjnego systemu RIS.

Szczegółowe wymagania dotyczące lokalizacji, parametrów pomiarowych, sposobu montażu, transmisji danych, zasilania, podgrzewania, diagnostyki, integracji z systemem RIS, tras kablowych, dokumentacji, testów, odbiorów, gwarancji, serwisu i utrzymania określają dalsze rozdziały PFU, w szczególności rozdział 1.2.7 oraz rozdziały dotyczące infrastruktury teletechnicznej terenowej, obiektów wieżowych, transmisji danych, zasilania, monitoringu technicznego, dokumentacji, testów i przekazania do eksploatacji.

1.1.2.6. Wieże, maszty, konstrukcje wsporcze i infrastruktura teletechniczna

Realizacja przedmiotu zamówienia obejmuje zaprojektowanie, wykonanie, dostawę, montaż, wyposażenie, uruchomienie, przetestowanie i przekazanie do eksploatacji infrastruktury terenowej systemu RIS stanowiącej platformę techniczną dla urządzeń instalowanych w nowych oraz modernizowanych lokalizacjach systemu RIS.

Infrastruktura ta obejmuje w szczególności obiekty wieżowe stacji radiokomunikacyjnych VHF/AIS/DGNSS, maszty, słupy kamerowe, konstrukcje wsporcze, konstrukcje montażowe, wsporniki, wysięgniki, uchwyty, elementy prowadzenia torów antenowych i kablowych, szafy teletechniczne typu zewnętrznego, fundamenty, ogrodzenia, zabezpieczenia techniczne, elementy dostępu serwisowego oraz inne elementy niezbędne do prawidłowego montażu, zasilania, zabezpieczenia, transmisji danych, eksploatacji i utrzymania urządzeń terenowych systemu RIS.

W ramach tej części przedmiotu zamówienia przewiduje się w szczególności wykonanie 8 nowych obiektów wieżowych stacji radiokomunikacyjnych VHF/AIS wraz z funkcją DGNSS, przeznaczonych również do instalacji sensorów meteorologicznych, kamer obserwacyjnych lub dozorowych, anten transmisyjnych, torów antenowych, urządzeń pomocniczych oraz elementów ochrony odgromowej i uziemiającej. Obiekty wieżowe będą stanowiły podstawową platformę techniczną dla urządzeń wymagających wyniesienia na wysokość w celu uzyskania wymaganych parametrów funkcjonalnych, propagacyjnych, obserwacyjnych, pomiarowych lub transmisyjnych.

Zakres tej części zamówienia obejmuje również wykonanie infrastruktury wsporczej i teletechnicznej dla lokalizacji, w których urządzenia systemu RIS będą instalowane na

obiektach mostowych, obiektach hydrotechnicznych, słupach kamerowych, istniejących konstrukcjach budowlanych albo innych konstrukcjach zaakceptowanych w dokumentacji projektowej. Dotyczy to w szczególności kamer monitoringu wizyjnego, czujników hydrologicznych, anten i urządzeń transmisji danych, elementów okablowania, urządzeń zasilających, zabezpieczeń oraz urządzeń monitoringu technicznego.

Szafy teletechniczne typu zewnętrznego będą stanowiły terenowe punkty instalacji, zasilania, ochrony, integracji i monitorowania urządzeń aktywnych oraz towarzyszących. Będą one wykorzystywane w szczególności w lokalizacjach wieżowych, mostowych, hydrotechnicznych, słupowych i terenowych, w których wymagane jest zapewnienie całorocznej eksploatacji urządzeń w warunkach zewnętrznych oraz ich integracji z systemem transmisji danych i systemem monitorowania zasobów RIS.

Infrastruktura terenowa objęta niniejszym rozdziałem ma charakter wspólny i przekrojowy dla kilku podsystemów systemu RIS. Będzie ona wykorzystywana przez system łączności radiowej VHF/AIS/DGNSS, system monitoringu wizyjnego CCTV, sieć połączeń transmisyjnych, czujniki hydrologiczne, sensory meteorologiczne, urządzenia zasilania, ochrony odgromowej i przepięciowej, monitoring techniczny oraz urządzenia pomocnicze niezbędne do prawidłowego funkcjonowania lokalizacji terenowych systemu RIS.

Zadaniem Generalnego Wykonawcy będzie zaprojektowanie każdej lokalizacji terenowej jako kompletnego punktu infrastruktury RIS, obejmującego nie tylko urządzenia właściwe dla danego podsystemu, lecz także niezbędne elementy konstrukcyjne, montażowe, teletechniczne, kablowe, zasilające, zabezpieczające, transmisyjne, serwisowe i eksploatacyjne. Rozwiązania te muszą być spójne z funkcją danej lokalizacji w systemie RIS oraz z wymaganiami wynikającymi z planów branżowych i dalszych części PFU.

Dobór rodzaju konstrukcji, sposobu posadowienia, sposobu mocowania urządzeń, przebiegu tras kablowych, lokalizacji szaf teletechnicznych, sposobu zasilania, ochrony odgromowej, uziemienia, zabezpieczenia przepięciowego, zabezpieczenia antykorozyjnego i dostępu serwisowego będzie podlegał doprecyzowaniu na etapie dokumentacji projektowej. Generalny Wykonawca zobowiązany będzie uwzględnić w szczególności warunki lokalne, uwarunkowania formalnoprawne, wymagania właścicieli i zarządców nieruchomości lub obiektów, warunki gruntowo-wodne, warunki zalewowe, oddziaływanie wiatru, oblodzenia, wilgoci, drgań, promieniowania UV oraz podwyższonej korozyjności środowiska.

W przypadku obiektów mostowych, hydrotechnicznych, drogowych, kolejowych albo innych obiektów istniejących Generalny Wykonawca będzie zobowiązany uwzględnić ich funkcję podstawową, stan techniczny, ograniczenia konstrukcyjne, wymagania zarządców, wymagania bezpieczeństwa, możliwość prowadzenia prac montażowych i serwisowych oraz wpływ planowanej infrastruktury RIS na eksploatację danego obiektu.

Realizacja tej części zamówienia obejmuje również wykonanie niezbędnej dokumentacji projektowej, uzgodnieniowej, wykonawczej, powykonawczej, odbiorowej i eksploatacyjnej dla infrastruktury terenowej, w tym dokumentacji dotyczącej konstrukcji, fundamentów, mocowań, tras kablowych, zasilania, uziemienia, ochrony odgromowej, ochrony przepięciowej, zabezpieczeń technicznych, dostępu serwisowego oraz powiązań z urządzeniami systemu RIS.

Szczegółowe wymagania techniczne dotyczące obiektów wieżowych stacji radiokomunikacyjnych, słupów kamerowych, szaf teletechnicznych typu zewnętrznego oraz

konstrukcji wsporczych określono w rozdziale 1.2.8 niniejszego PFU. Wymagania te należy stosować łącznie z wymaganiami właściwymi dla poszczególnych podsystemów RIS, w szczególności dla systemu łączności radiowej VHF/AIS/DGNSS, systemu monitoringu wizyjnego CCTV, sieci połączeń transmisyjnych, czujników hydrologicznych, sensorów meteorologicznych, zasilania, cyberbezpieczeństwa, dokumentacji, testów, odbiorów, gwarancji, serwisu i utrzymania.

1.1.2.7. Doposażenie serwerowni głównej systemu RIS

Przedmiot zamówienia obejmuje doposażenie serwerowni głównej systemu RIS w zakresie niezbędnym do obsługi rozbudowanego środowiska usług informacji rzecznej na Odrzańskiej Drodze Wodnej. Zakres ten obejmuje dostawę, instalację, konfigurację, uruchomienie, integrację, przetestowanie i przekazanie do eksploatacji wybranych komponentów infrastruktury serwerowej, sieciowej, pamięci masowej oraz systemu kopii zapasowych.

Doposażenie serwerowni głównej jest powiązane z rozbudową systemu RIS o nowe lokalizacje terenowe, nowe źródła danych, nowe strumienie wideo, nowe usługi cyfrowe, usługi VTT, usługi informacji hydrometeorologicznej, mechanizmy integracji danych oraz mechanizmy monitorowania zasobów infrastrukturalnych i aplikacyjnych systemu. Celem tej części zamówienia jest zapewnienie, aby warstwa centralna systemu RIS posiadała odpowiednie zasoby techniczne do przyjmowania, przetwarzania, przechowywania, zabezpieczania i udostępniania danych pochodzących z rozbudowywanego systemu.

Punktem wyjścia dla tej części zamówienia jest istniejące środowisko serwerowni głównej systemu RIS, obejmujące w szczególności środowisko serwerów kasetowych Dell EMC PowerEdge MX7000 z serwerami kasetowymi Dell EMC PowerEdge MX740c, macierz dyskową Dell EMC PowerVault ME4024 oraz rozwiązanie Dell EMC Avamar DP4400 / Integrated Data Protection Appliance / PowerProtect DP4400. Doposażenie musi zostać wykonane z zachowaniem kompatybilności z istniejącą architekturą techniczną, zasadami eksploatacji, konfiguracją środowiska, politykami bezpieczeństwa oraz wymaganiami ciągłości działania.

Zakres doposażenia serwerowni głównej obejmuje w szczególności:

1) rozbudowę wyposażenia sieciowego serwerów kasetowych, w tym dostawę i uruchomienie dodatkowych kart sieciowych dla serwerów Dell EMC PowerEdge MX740c, w celu rozdzielenia ruchu DATA od ruchu SAN / storage oraz zwiększenia możliwości konfiguracji i optymalizacji transmisji danych w środowisku serwerowym;
2) rozbudowę macierzy dyskowej Dell EMC PowerVault ME4024, w tym dostawę, instalację, konfigurację i uruchomienie dodatkowych zasobów pamięci masowej, niezbędnych do obsługi zwiększonego wolumenu danych systemu RIS;
3) rozbudowę rozwiązania Dell EMC Avamar DP4400 / Integrated Data Protection Appliance / PowerProtect DP4400, w tym zwiększenie dostępnej pojemności środowiska kopii zapasowych oraz zapewnienie wymaganych licencji, konfiguracji i wsparcia producenta;
4) wykonanie niezbędnych prac integracyjnych w istniejącym środowisku serwerowni głównej, w tym w zakresie konfiguracji sieci, storage, backupu, wirtualizacji, systemów zarządzania, monitoringu i bezpieczeństwa;

5) przeprowadzenie testów potwierdzających poprawność instalacji, konfiguracji, wydajności, dostępności, rozdzielenia ruchu, działania mechanizmów wysokiej dostępności, poprawności wykonywania kopii zapasowych oraz możliwości odtworzenia danych;
6) opracowanie i przekazanie dokumentacji powykonawczej, konfiguracyjnej, administracyjnej, eksploatacyjnej, licencyjnej, gwarancyjnej i odbiorowej;
7) zapewnienie gwarancji, wsparcia producenta, aktualizacji oraz przekazania rozwiązania do utrzymania przez Zamawiającego.

Doposażenie serwerowni głównej musi zostać wykonane jako rozbudowa istniejącego środowiska produkcyjnego systemu RIS, a nie jako odrębne, izolowane rozwiązanie infrastrukturalne. Oznacza to, że wszystkie dostarczane komponenty muszą zostać zintegrowane z obecnie eksploatowaną architekturą serwerową, sieciową, pamięci masowej, kopii zapasowych, monitoringu, bezpieczeństwa i zarządzania.

Realizacja prac w serwerowni głównej musi uwzględniać konieczność utrzymania ciągłości działania systemu RIS. Generalny Wykonawca zobowiązany jest zaplanować prace w sposób ograniczający ryzyko przerw w dostępności usług, utraty danych, pogorszenia parametrów pracy albo utraty wsparcia producenta dla istniejących komponentów. Prace ingerujące w środowisko produkcyjne muszą być realizowane w uzgodnionych z Zamawiającym oknach serwisowych.

Szczegółowe wymagania dotyczące rozbudowy kart sieciowych w serwerach kasetowych, rozbudowy macierzy dyskowej, rozbudowy rozwiązania kopii zapasowych, kompatybilności, instalacji, konfiguracji, testów, dokumentacji, gwarancji, wsparcia producenta, bezpieczeństwa i realizacji prac w środowisku produkcyjnym określono w rozdziale 1.2.12 Wymagania dla doposażenia serwerowni głównej.

1.1.2.8. Modernizacja pomieszczenia serwerowni pełniącej rolę węzła telekomunikacyjnego

Przedmiot zamówienia obejmuje modernizację pomieszczenia serwerowni pełniącej funkcję węzła telekomunikacyjnego systemu RIS, zlokalizowanego w pomieszczeniu nr 32 na parterze siedziby Zamawiającego w budynku tzw. Czerwonego Ratusza przy Placu Batorego 4 w Szczecinie.

Pomieszczenie w zakresie pełnionej roli węzła telekomunikacyjnego to zostało wykonane w ramach wcześniejszego, pilotażowego wdrożenia systemu RIS Dolnej Odra i jest obecnie wykorzystywane jako element infrastruktury technicznej Zamawiającego, w szczególności jako węzeł sieci LAN/WAN oraz miejsce instalacji wybranych zasobów teleinformatycznych i backupowych systemu RIS. W ramach niniejszego zamówienia pomieszczenie to ma zostać dostosowane do aktualnych i docelowych potrzeb eksploatacyjnych zmodernizowanego systemu RIS.

Celem modernizacji jest podniesienie bezpieczeństwa, niezawodności, odporności środowiskowej i eksploatacyjnej pomieszczenia pełniącego funkcję węzła telekomunikacyjnego, a także zapewnienie jego prawidłowego powiązania z serwerownią główną, modernizowaną

siecią teleinformatyczną Zamawiającego, systemami zasilania, systemami bezpieczeństwa technicznego oraz systemem monitorowania zasobów infrastrukturalnych systemu RIS.

Zakres tej części przedmiotu zamówienia obejmuje w szczególności zaprojektowanie, wykonanie, dostawę, montaż, konfigurację, uruchomienie, przetestowanie i przekazanie do eksploatacji rozwiązań niezbędnych do modernizacji pomieszczenia nr 32 jako pomieszczenia technicznego pełniącego funkcję węzła telekomunikacyjnego.

Główne obszary modernizacji obejmują w szczególności:

1) modernizację układu zasilania pomieszczenia, w tym jego powiązanie z docelowym systemem zasilania serwerowni głównej oraz układami zasilania podstawowego, rezerwowego i awaryjnego Zamawiającego;
2) wymianę podłogi technicznej / podłogi podwyższonej, z uwzględnieniem wymagań odporności ogniowej, nośności, prowadzenia instalacji, dostępu serwisowego i bezpieczeństwa eksploatacyjnego;
3) wykonanie systemu wczesnego wykrywania pożaru, dostosowanego do charakteru pomieszczenia technicznego oraz znajdujących się w nim urządzeń teleinformatycznych;
4) wykonanie systemu gaszenia, dobranego do pomieszczenia technicznego oraz urządzeń teleinformatycznych, w sposób ograniczający ryzyko uszkodzenia infrastruktury IT;
5) wykonanie systemu monitorowania parametrów środowiskowych pomieszczenia, w szczególności temperatury, wilgotności, zasilania, zdarzeń alarmowych i innych parametrów mających wpływ na bezpieczeństwo pracy urządzeń;
6) wymianę urządzeń klimatyzacyjnych, w sposób zapewniający utrzymanie właściwych warunków środowiskowych dla urządzeń zainstalowanych w pomieszczeniu;
7) uporządkowanie i dostosowanie infrastruktury kablowej, tras kablowych, przepustów, połączeń teleinformatycznych, połączeń zasilających, uziemienia i połączeń wyrównawczych;
8) dostosowanie pomieszczenia do pełnienia funkcji punktu koncentracji dla części modernizowanej sieci teleinformatycznej Zamawiającego;
9) integrację elementów technicznych pomieszczenia z systemem monitoringu technicznego zasobów infrastrukturalnych i aplikacyjnych systemu RIS;
10) wykonanie dokumentacji projektowej, wykonawczej, powykonawczej, konfiguracyjnej, eksploatacyjnej i odbiorowej dla wszystkich elementów objętych modernizacją.

Modernizacja pomieszczenia nr 32 musi zostać skoordynowana z pozostałymi zadaniami realizowanymi w ramach zamówienia, w szczególności z doposażeniem serwerowni głównej systemu RIS, modernizacją sieci teleinformatycznej w siedzibie Zamawiającego, utworzeniem serwerowni zapasowej, rozbudową sieci transmisji danych oraz wdrożeniem monitoringu technicznego zasobów systemu RIS.

Generalny Wykonawca zobowiązany będzie prowadzić prace w sposób zapewniający ograniczenie ryzyka przerw w działaniu istniejącej infrastruktury teleinformatycznej Zamawiającego. W przypadku konieczności czasowego wyłączenia urządzeń, łączy, zasilania,

klimatyzacji, systemów zabezpieczeń albo innych elementów wpływających na ciągłość działania systemu RIS, prace muszą zostać zaplanowane, uzgodnione z Zamawiającym i wykonane w zaakceptowanym oknie serwisowym.

Realizacja zadania obejmuje również weryfikację stanu istniejącego pomieszczenia, istniejących instalacji, urządzeń, tras kablowych, punktów zasilania, systemów bezpieczeństwa, klimatyzacji, podłogi technicznej, uziemienia, połączeń wyrównawczych oraz powiązań z pozostałą infrastrukturą teleinformatyczną Zamawiającego. Wyniki tej weryfikacji muszą zostać uwzględnione w dokumentacji projektowej.

Modernizowane pomieszczenie musi zostać przekazane Zamawiającemu jako kompletne, bezpieczne, uporządkowane, udokumentowane i przygotowane do dalszej eksploatacji pomieszczenie techniczne pełniące funkcję węzła telekomunikacyjnego systemu RIS.

Szczegółowe wymagania Zamawiającego dotyczące modernizacji pomieszczenia serwerowni pełniącej rolę węzła telekomunikacyjnego określono w rozdziale 1.2.10 „Wymagania dla modernizacji serwerowni”.

1.1.2.9. Modernizacja sieci teleinformatycznej

Przedmiot zamówienia obejmuje modernizację części sieci teleinformatycznej w siedzibie Zamawiającego, zlokalizowanej w budynku tzw. Czerwonego Ratusza. Zakres zadania dotyczy wykonania nowej instalacji teleinformatycznej oraz powiązanej infrastruktury punktów elektryczno-logicznych w zachodnim skrzydle budynku, w pomieszczeniach położonych na parterze.

Modernizacja obejmuje następujące pomieszczenia: 19A, 20, 23A, 23B, 23C, 24, 25, 26, 27, 28, 29, 29A, 29B, 30 oraz 31. Łącznie zakresem zadania objętych jest 15 pomieszczeń. Rozlokowanie pomieszczeń objętych modernizacją przedstawiono na rysunku zamieszczonym w Załączniku nr 1..

Celem tej części zamówienia jest wykonanie uporządkowanej, nowej, strukturalnej sieci teleinformatycznej w kategorii 6, umożliwiającej obsługę stanowisk pracy, urządzeń sieciowych, urządzeń końcowych oraz dodatkowych punktów logicznych przeznaczonych do zasilania i komunikacji z tabletami informacyjnymi instalowanymi przy wejściach do pomieszczeń.

W ramach zadania Generalny Wykonawca zobowiązany będzie wykonać w każdym z pomieszczeń po dwa punkty elektryczno-logiczne, zwane dalej PEL, z zastrzeżeniem wyjątków wskazanych poniżej. Każdy PEL musi obejmować dwa gniazda zasilające w standardzie Schuko oraz dwa punkty logiczne zakończone złączem RJ45.

Wyjątek od podstawowego założenia dwóch PEL w pomieszczeniu dotyczy pomieszczenia nr 30, w którym należy wykonać cztery punkty PEL. Dodatkowo w pomieszczeniu nr 29B, pełniącym funkcję sali konferencyjnej, Generalny Wykonawca zobowiązany będzie wykonać jeden dodatkowy punkt PEL osadzony w podłodze pod stołem konferencyjnym, przeznaczony do obsługi urządzeń wykorzystywanych w ramach pracy konferencyjnej i spotkaniowej.

Minimalny zakres ilościowy zadania obejmuje wykonanie łącznie 33 punktów PEL, w tym:

1) po dwa punkty PEL w pomieszczeniach: 19A, 20, 23A, 23B, 23C, 24, 25, 26, 27, 28, 29, 29A, 29B oraz 31;
2) cztery punkty PEL w pomieszczeniu nr 30;
3) jeden dodatkowy punkt PEL osadzony w podłodze pod stołem konferencyjnym w pomieszczeniu nr 29B.

Ponieważ każdy PEL obejmuje dwa gniazda zasilające w standardzie Schuko oraz dwa punkty logiczne RJ45, minimalny zakres ilościowy w tym obszarze obejmuje wykonanie 66 gniazd zasilających oraz 66 punktów logicznych RJ45 związanych z punktami PEL.

Dodatkowo w każdym pomieszczeniu należy wykonać jeden dodatkowy punkt logiczny, zlokalizowany w pobliżu drzwi wejściowych do pomieszczenia. Punkty te będą przeznaczone do podłączenia tabletów informacyjnych zasilanych z wykorzystaniem standardu PoE. Minimalny zakres ilościowy w tym obszarze obejmuje wykonanie 15 dodatkowych punktów logicznych RJ45 z możliwością wykorzystania do zasilania urządzeń końcowych w standardzie PoE.

Łącznie minimalny zakres logiczny modernizowanej instalacji obejmuje wykonanie 81 punktów logicznych RJ45, w tym 66 punktów logicznych w ramach punktów PEL oraz 15 dodatkowych punktów logicznych przeznaczonych dla tabletów informacyjnych.

Punktem koncentracji sieci dla pomieszczeń 19A oraz 20 będzie pomieszczenie serwerowni głównej Zamawiającego. Dla pozostałych pomieszczeń objętych zakresem modernizacji punktem koncentracji będzie pomieszczenie serwerowni pełniącej funkcję węzła telekomunikacyjnego, która podlega modernizacji w ramach realizacji niniejszego zamówienia.

Zakres tej części zamówienia obejmuje również dostawę, montaż, konfigurację, uruchomienie i przekazanie do eksploatacji urządzeń aktywnych niezbędnych do obsługi modernizowanej sieci teleinformatycznej, w tym co najmniej dwóch przełączników dostępowych PoE o liczbie 48 portów każdy albo odpowiedniej wielokrotności przełączników PoE o liczbie 24 portów każdy, zapewniającej nie mniejszą łączną liczbę dostępnych portów oraz wymaganą funkcjonalność eksploatacyjną.

Dostarczone przełączniki PoE muszą umożliwiać obsługę punktów logicznych modernizowanej sieci, w tym punktów przeznaczonych do podłączenia tabletów informacyjnych zasilanych z wykorzystaniem standardu PoE, oraz zapewniać możliwość integracji z istniejącą infrastrukturą sieciową Zamawiającego. Generalny Wykonawca zobowiązany jest dostarczyć komplet okablowania sygnałowego, kabli połączeniowych, wkładek, modułów, przewodów krosowych, elementów stakujących albo innych elementów wymaganych do połączenia przełączników w stos oraz do ich podłączenia do przełączników szkieletowych pracujących w układzie pary niezawodnościowej Dell S5224F-ON 24x 25GbE SFP eksploatowanych przez Zamawiającego.

Dostawa urządzeń aktywnych musi obejmować również wszystkie niezbędne licencje, akcesoria montażowe, elementy zasilania, przewody, moduły transmisyjne, konfigurację, oznakowanie, dokumentację powykonawczą, dokumentację konfiguracyjną, wykonanie testów połączeń, weryfikację poprawności pracy portów PoE, weryfikację połączenia z warstwą szkieletową oraz przekazanie urządzeń do eksploatacji w ramach infrastruktury sieciowej Zamawiającego.

Wykonanie sieci teleinformatycznej musi zostać skoordynowane z modernizacją pomieszczenia serwerowni pełniącej funkcję węzła telekomunikacyjnego, z istniejącą infrastrukturą teleinformatyczną Zamawiającego, z organizacją pracy w budynku oraz z wymaganiami dotyczącymi bezpieczeństwa, estetyki, ochrony przeciwpożarowej, prowadzenia tras kablowych i minimalizacji ingerencji w istniejącą substancję budowlaną.

Realizacja zadania obejmuje w szczególności zaprojektowanie przebiegu tras kablowych, wykonanie okablowania strukturalnego, montaż punktów PEL, montaż dodatkowych punktów logicznych dla tabletów informacyjnych, wykonanie podłogowego punktu PEL w sali konferencyjnej, wykonanie zakończeń kablowych, oznakowanie punktów i kabli, dostawę, montaż i konfigurację przełączników dostępowych PoE, dostarczenie okablowania i elementów niezbędnych do połączenia przełączników w stos oraz ich podłączenia do przełączników szkieletowych Zamawiającego, włączenie instalacji do właściwych punktów koncentracji, wykonanie pomiarów, testów, dokumentacji powykonawczej oraz przekazanie instalacji do eksploatacji.

Modernizowana sieć teleinformatyczna musi zostać wykonana jako element infrastruktury technicznej Zamawiającego, wspierający funkcjonowanie środowiska pracy, systemów teleinformatycznych, usług cyfrowych oraz infrastruktury RIS. Rozwiązanie musi umożliwiać bezpieczną i uporządkowaną eksploatację, identyfikację punktów, dalszą administrację, diagnostykę, utrzymanie i ewentualną rozbudowę.

Szczegółowe wymagania dotyczące kategorii okablowania, sposobu prowadzenia tras kablowych, punktów PEL, punktów logicznych PoE, podłogowego punktu PEL w sali konferencyjnej, zakończeń kablowych, punktów koncentracji, pomiarów, oznakowania, dokumentacji, odbioru i warunków realizacji prac określono w rozdziale 1.2.11. Wymagania dla modernizacji sieci teleinformatycznej.

1.1.2.10. Środowisko pracy zmodernizowanego systemu RIS

W ramach realizacji przedmiotu zamówienia Generalny Wykonawca zobowiązany będzie do zaprojektowania, dostarczenia, wdrożenia, skonfigurowania, uruchomienia, przetestowania i przekazania do eksploatacji nowego środowiska pracy zmodernizowanego systemu RIS, zapewniającego prawidłowe funkcjonowanie usług, aplikacji, baz danych, komponentów integracyjnych, systemów operatorskich, systemów monitorowania, usług cyfrowych oraz pozostałych komponentów systemu RIS objętych niniejszym zamówieniem.

Środowisko pracy zmodernizowanego systemu RIS musi zostać zaprojektowane jako rozwiązanie dwulokalizacyjne, obejmujące co najmniej:

1) lokalizację podstawową, zlokalizowaną w siedzibie Zamawiającego jako podstawowe centrum przetwarzania danych systemu RIS;
2) lokalizację zapasową, pełniącą funkcję zapasowego centrum przetwarzania danych systemu RIS, której wybór, przygotowanie w zakresie niezbędnym do uruchomienia środowiska oraz połączenie z lokalizacją podstawową stanowią element przedmiotu zamówienia.

Utworzenie środowiska pracy zmodernizowanego systemu RIS stanowi odrębny zakres rzeczowy projektu względem zadań polegających na doposażeniu serwerowni głównej systemu RIS. Oznacza to, że Generalny Wykonawca nie może ograniczyć tego zadania wyłącznie do dostawy pojedynczych urządzeń, rozbudowy istniejących zasobów serwerowni głównej albo instalacji komponentów infrastrukturalnych w jednej lokalizacji. Rezultatem realizacji tego zadania ma być kompletne, uruchomione, przetestowane i gotowe do eksploatacji środowisko pracy systemu RIS, działające w oparciu o dwie lokalizacje przetwarzania danych.

Celem budowy nowego środowiska pracy zmodernizowanego systemu RIS jest zapewnienie odpowiedniej dostępności, wydajności, skalowalności, bezpieczeństwa, odporności na awarie oraz możliwości odtworzenia działania systemu RIS w przypadku awarii pojedynczego komponentu, awarii grupy komponentów albo niedostępności jednej z lokalizacji przetwarzania danych. Środowisko musi umożliwiać utrzymanie ciągłości działania usług krytycznych systemu RIS oraz bezpieczne i kontrolowane odtworzenie działania systemu zgodnie z wymaganiami określonymi w PFU, Planie Ciągłości Działania BCP, Planie Odtworzenia po Awarii DRP oraz dokumentacji projektowej i powykonawczej opracowanej przez Generalnego Wykonawcę.

Środowisko pracy zmodernizowanego systemu RIS musi obejmować wszystkie warstwy techniczne niezbędne do prawidłowego funkcjonowania systemu, w szczególności:

1) warstwę obliczeniową, obejmującą serwery, platformę wirtualizacyjną, klastry niezawodnościowe, zasoby obliczeniowe dla usług aplikacyjnych, bazodanowych, integracyjnych, operatorskich, monitorujących, raportowych i administracyjnych;
2) warstwę składowania danych, obejmującą zasoby pamięci masowej wymagane dla baz danych, systemów aplikacyjnych, komponentów integracyjnych, systemów monitorowania, repozytoriów technicznych, konfiguracji, logów oraz danych systemu RIS;
3) warstwę sieci LAN, obejmującą komunikację wewnętrzną komponentów środowiska w lokalizacji podstawowej i lokalizacji zapasowej;
4) warstwę SAN albo równoważną warstwę komunikacji z zasobami pamięci masowej, jeżeli przyjęta przez Generalnego Wykonawcę architektura będzie tego wymagała;
5) warstwę połączenia między lokalizacją podstawową i lokalizacją zapasową;
6) warstwę kopii zapasowych, replikacji i odtworzenia po awarii;
7) warstwę bezpieczeństwa, obejmującą segmentację, kontrolę dostępu, szyfrowanie transmisji, zarządzanie uprawnieniami, logowanie, monitoring bezpieczeństwa i ochronę administracyjnego dostępu do zasobów;
8) warstwę monitoringu technicznego i zarządzania, obejmującą monitorowanie dostępności, wydajności, pojemności, stanu usług, stanu komponentów infrastrukturalnych, zdarzeń technicznych, alarmów, kopii zapasowych, replikacji i połączeń między lokalizacjami;
9) warstwę integracji ze środowiskami, usługami, siecią transmisji danych, systemami operatorskimi, systemem CCTV, VHF/AIS/DGNSS, czujnikami hydrologicznymi, sensorami meteorologicznymi, usługami cyfrowymi RIS oraz systemami zewnętrznymi.

Generalny Wykonawca zobowiązany jest zaprojektować środowisko pracy zmodernizowanego systemu RIS w sposób kompletny, spójny i dostosowany do rzeczywistych potrzeb systemu RIS. W szczególności Generalny Wykonawca zobowiązany jest dobrać liczbę, typy, parametry techniczne oraz sposób konfiguracji serwerów, przełączników SAN, przełączników LAN, urządzeń bezpieczeństwa, urządzeń transmisyjnych, urządzeń zarządzających, elementów połączeniowych, kart rozszerzeń, wkładek optycznych, kabli, modułów, licencji, subskrypcji, systemów operacyjnych, platform wirtualizacyjnych, mechanizmów replikacji, backupu i monitoringu oraz innych elementów niezbędnych do osiągnięcia wymaganej funkcjonalności i parametrów środowiska.

Dobór liczby i typów przełączników SAN, przełączników LAN oraz innych urządzeń aktywnych niezbędnych do zapewnienia komunikacji komponentów środowiska w ramach każdej lokalizacji oraz pomiędzy lokalizacjami należy do obowiązków Generalnego Wykonawcy. Dobór ten musi zostać wykonany z uwzględnieniem zasobów posiadanych przez Zamawiającego, planowanego sposobu wykorzystania istniejącej infrastruktury, wymagań dotyczących wydajności, dostępności, bezpieczeństwa, separacji ruchu, replikacji, backupu, zarządzania, monitoringu oraz możliwości dalszej rozbudowy środowiska.

Generalny Wykonawca zobowiązany jest przeprowadzić analizę istniejących zasobów Zamawiającego, które mogą zostać wykorzystane na potrzeby budowy środowiska pracy zmodernizowanego systemu RIS. Analiza ta musi obejmować co najmniej zasoby serwerowe, macierzowe, sieciowe, transmisyjne, zabezpieczające, backupowe, wirtualizacyjne, licencyjne, energetyczne, klimatyzacyjne, szafowe oraz organizacyjne. W dokumentacji projektowej Generalny Wykonawca musi jednoznacznie wskazać, które zasoby Zamawiającego zostaną wykorzystane, które zostaną rozbudowane, które zostaną zintegrowane z nowym środowiskiem, które pozostaną bez zmian oraz jakie nowe zasoby muszą zostać dostarczone w ramach zamówienia.

Środowisko pracy zmodernizowanego systemu RIS musi zostać zaprojektowane jako środowisko wysokiej dostępności, eliminujące pojedyncze punkty awarii w zakresie adekwatnym do przyjętej architektury. Dotyczy to w szczególności zasilania, połączeń sieciowych, połączeń SAN albo równoważnych, adapterów serwerowych, kontrolerów pamięci masowej, urządzeń sieciowych, urządzeń bezpieczeństwa, elementów transmisji między lokalizacjami, platformy wirtualizacyjnej, usług zarządzających, mechanizmów replikacji, mechanizmów backupu i monitoringu.

Środowisko musi umożliwiać pracę w modelu zapewniającym przejęcie działania przez lokalizację zapasową w przypadku niedostępności lokalizacji podstawowej, zgodnie z przyjętym i zaakceptowanym przez Zamawiającego wariantem architektury. Dopuszczalne jest zastosowanie modelu aktywno-zapasowego albo innego modelu architektonicznego zapewniającego równoważny albo wyższy poziom dostępności, pod warunkiem wykazania przez Generalnego Wykonawcę, że przyjęte rozwiązanie spełnia wymagania PFU, jest możliwe do utrzymania przez Zamawiającego oraz nie powoduje nadmiernej złożoności eksploatacyjnej.

W ramach systemu RIS nie przewiduje się dostawy i wdrożenia macierzy NAS ani bibliotek taśmowych. Generalny Wykonawca nie powinien projektować środowiska w oparciu o obowiązkowe zastosowanie takich komponentów. Jeżeli Generalny Wykonawca uzna, że dla osiągnięcia określonej funkcjonalności konieczne jest zastosowanie równoważnych mechanizmów składowania plikowego, repozytoriów danych, archiwizacji lub backupu, musi

zapewnić ich realizację w ramach dostarczanych albo wykorzystywanych komponentów środowiska, bez wprowadzania macierzy NAS i bibliotek taśmowych jako wymaganych elementów dostawy.

Wybór lokalizacji zapasowego centrum przetwarzania danych systemu RIS należy do zakresu odpowiedzialności Generalnego Wykonawcy. Generalny Wykonawca zobowiązany jest wskazać, uzasadnić i uzgodnić z Zamawiającym lokalizację zapasową, uwzględniając wymagania dostępności, bezpieczeństwa fizycznego i teleinformatycznego, warunków środowiskowych, zasilania, klimatyzacji, ochrony przeciwpożarowej, kontroli dostępu, możliwości instalacji infrastruktury, możliwości zapewnienia łączności z lokalizacją podstawową, dostępności serwisowej, kosztów eksploatacyjnych oraz trwałości rozwiązania w okresie wymaganym dla projektu.

Generalny Wykonawca zobowiązany jest zaprojektować, wybudować, uruchomić i przetestować medium transmisyjne łączące zapasowe centrum przetwarzania danych z siedzibą Zamawiającego. Medium to musi zapewniać parametry przepustowości, opóźnień, dostępności, bezpieczeństwa i niezawodności odpowiednie dla przyjętej architektury środowiska, w szczególności dla replikacji danych, synchronizacji komponentów, mechanizmów HA, backupu, odtwarzania po awarii, monitoringu, zarządzania oraz komunikacji usług systemu RIS. Dobór technologii połączenia, przebiegu, parametrów oraz wymaganych urządzeń aktywnych i pasywnych należy do Generalnego Wykonawcy i wymaga akceptacji Zamawiającego.

Środowisko pracy zmodernizowanego systemu RIS musi zostać zaprojektowane z uwzględnieniem docelowego sposobu działania wszystkich istotnych komponentów systemu RIS, w szczególności usług VTT, usług informacji hydrologicznej i meteorologicznej, usług cyfrowych RIS, systemów operatorskich, systemów integracyjnych, baz danych, API, systemów monitoringu wizyjnego CCTV, systemów VHF/AIS/DGNSS, usług transmisji danych, monitoringu technicznego oraz mechanizmów udostępniania danych interesariuszom zewnętrznym.

Generalny Wykonawca zobowiązany jest zapewnić, aby środowisko pracy systemu RIS było skalowalne i umożliwiało rozbudowę zasobów obliczeniowych, pamięci masowej, przepustowości sieciowej, liczby maszyn wirtualnych, liczby usług, liczby integracji, zakresu danych oraz mechanizmów monitoringu bez konieczności przebudowy zasadniczej architektury. Skalowalność środowiska musi być zapewniona zarówno w lokalizacji podstawowej, jak i zapasowej, z uwzględnieniem ograniczeń wynikających z dostępnej powierzchni, zasilania, chłodzenia, szaf rack, licencji i połączeń między lokalizacjami.

Środowisko musi zostać zaprojektowane w sposób umożliwiający centralne zarządzanie, monitorowanie, aktualizowanie, wykonywanie kopii zapasowych, odtwarzanie, dokumentowanie zmian oraz obsługę incydentów technicznych i bezpieczeństwa. Wszystkie kluczowe komponenty środowiska muszą być objęte monitoringiem technicznym i logowaniem zdarzeń. Monitoring musi obejmować co najmniej dostępność usług, stan komponentów infrastrukturalnych, wykorzystanie zasobów, stan replikacji, stan backupu, stan połączenia między lokalizacjami, zdarzenia bezpieczeństwa, alarmy krytyczne oraz zdarzenia wpływające na ciągłość działania systemu RIS.

Środowisko pracy zmodernizowanego systemu RIS musi zostać zintegrowane z projektowaną i istniejącą siecią transmisji danych systemu RIS. Integracja ta musi uwzględniać segmentację logiczną, separację ruchu, adresację, reguły komunikacji, połączenia VPN, zasady

bezpieczeństwa, monitoring, diagnostykę, przepustowość, priorytetyzację ruchu, komunikację z lokalizacjami terenowymi oraz komunikację z systemami zewnętrznymi. Generalny Wykonawca zobowiązany jest zapewnić, aby nowe środowisko pracy systemu RIS nie powodowało niekontrolowanego wpływu na funkcjonowanie istniejącego systemu RIS oraz pozostałych systemów teleinformatycznych Zamawiającego.

W ramach realizacji zadania Generalny Wykonawca zobowiązany jest opracować kompletną dokumentację projektową, wdrożeniową, konfiguracyjną, testową, powykonawczą i eksploatacyjną środowiska pracy zmodernizowanego systemu RIS. Dokumentacja musi obejmować co najmniej opis architektury, opis lokalizacji, wykaz wykorzystanych zasobów Zamawiającego, wykaz dostarczonych zasobów, schematy logiczne i fizyczne, opis połączenia między lokalizacjami, opis konfiguracji sieci LAN i SAN albo równoważnej, opis konfiguracji wirtualizacji, opis konfiguracji pamięci masowej, opis mechanizmów replikacji, backupu, HA i DR, opis monitoringu, opis bezpieczeństwa, wykaz licencji, opis procedur administracyjnych oraz opis procedur awaryjnych.

Generalny Wykonawca zobowiązany jest przeprowadzić testy potwierdzające gotowość środowiska pracy zmodernizowanego systemu RIS do eksploatacji. Testy muszą obejmować co najmniej poprawność instalacji i konfiguracji, komunikację wewnątrz każdej lokalizacji, komunikację pomiędzy lokalizacjami, działanie mechanizmów wysokiej dostępności, działanie mechanizmów replikacji, wykonywanie i odtwarzanie kopii zapasowych, przełączenie pracy na lokalizację zapasową, powrót do lokalizacji podstawowej, monitoring, alarmowanie, bezpieczeństwo, wydajność, pojemność, skalowalność oraz współpracę środowiska z komponentami systemu RIS.

Generalny Wykonawca ponosi odpowiedzialność za osiągnięcie kompletnego rezultatu w postaci środowiska pracy zmodernizowanego systemu RIS gotowego do uruchomienia produkcyjnego i dalszej eksploatacji przez Zamawiającego. Odpowiedzialność Generalnego Wykonawcy obejmuje nie tylko dostawę sprzętu, oprogramowania, licencji i elementów połączeniowych, lecz także ich prawidłowy dobór, zaprojektowanie, instalację, konfigurację, integrację, testy, dokumentację, usunięcie niezgodności, przekazanie wiedzy administratorom Zamawiającego oraz zapewnienie wsparcia gwarancyjnego zgodnie z wymaganiami PFU i umowy.

1.1.2.11. Utworzenie serwerowni zapasowej oraz łącza teleinformatycznego łączącego ją z Centrum RIS

Przedmiot zamówienia obejmuje utworzenie serwerowni zapasowej systemu RIS na bazie zasobów zewnętrznego Data Center oraz zestawienie dedykowanego światłowodowego łącza teleinformatycznego pomiędzy serwerownią telekomunikacyjną Zamawiającego a lokalizacją zewnętrznego Data Center. Zakres ten ma zapewnić Zamawiającemu możliwość uruchomienia zapasowej lokalizacji infrastrukturalnej systemu RIS, przeznaczonej do obsługi funkcji replikacji danych, zabezpieczenia danych, odtworzenia pracy po awarii, wsparcia ciągłości działania oraz realizacji scenariuszy wynikających z Planu Ciągłości Działania i Planu Odtworzenia po Awarii.

Serwerownia zapasowa ma zostać zlokalizowana w zewnętrznym Data Center, położonym w odległości umożliwiającej efektywną realizację funkcji replikacji danych pomiędzy zasobami pamięci masowej zlokalizowanymi w serwerowni głównej Zamawiającego oraz zasobami zlokalizowanymi w ośrodku zapasowym. Lokalizacja Data Center musi umożliwiać realizację

funkcji zapasowych systemu RIS, przy zachowaniu wymagań dotyczących dostępności, bezpieczeństwa fizycznego, bezpieczeństwa teleinformatycznego, zasilania, chłodzenia, monitoringu, dostępu serwisowego oraz ciągłości świadczenia usług kolokacyjnych.

Zakres ilościowy tej części zamówienia obejmuje co najmniej:

1) utworzenie 1 ośrodka zapasowego systemu RIS w zewnętrznym Data Center;
2) zapewnienie 1 szafy teleinformatycznej typu RACK o wysokości 47U na potrzeby kolokacji zasobów infrastrukturalnych Zamawiającego;
3) zapewnienie przyłącza energetycznego dla szafy RACK wraz z układem pomiarowym, w tym licznikiem umożliwiającym rozliczanie kosztów zużycia energii elektrycznej;
4) zaprojektowanie i wykonanie 1 dedykowanego przyłącza światłowodowego 6J pomiędzy serwerownią telekomunikacyjną Zamawiającego a lokalizacją zewnętrznego Data Center;
5) wykonanie zakończeń światłowodowych w obu lokalizacjach;
6) wykonanie pomiarów, testów i uruchomienie połączenia pomiędzy wskazanymi lokalizacjami;
7) zapewnienie utrzymania, nadzoru technicznego, serwisu, usuwania awarii oraz dostępności łącza w okresie realizacji zamówienia oraz w okresie gwarancji po Odbiorze Końcowym;
8) zapewnienie finansowania przez Generalnego Wykonawcę kosztów najmu szafy teleinformatycznej, kosztów energii elektrycznej, kosztów utrzymania usługi transmisji danych oraz innych kosztów eksploatacyjnych wymaganych do działania ośrodka zapasowego w okresie realizacji zamówienia oraz w okresie gwarancji po Odbiorze Końcowym.

Budowa przyłącza światłowodowego 6J obejmuje kompleksowe wykonanie infrastruktury telekomunikacyjnej, w szczególności opracowanie dokumentacji projektowej, przeprowadzenie uzgodnień formalnoprawnych, uzyskanie wymaganych zgód i pozwoleń, wykonanie infrastruktury kablowej, dostarczenie i instalację kabla światłowodowego, wykonanie zakończeń światłowodowych, wykonanie pomiarów, uruchomienie połączenia oraz przekazanie kompletnej dokumentacji powykonawczej.

W wyniku realizacji zadania Zamawiający ma stać się właścicielem wybudowanego przyłącza światłowodowego 6J pomiędzy serwerownią telekomunikacyjną Zamawiającego a lokalizacją zewnętrznego Data Center, z zastrzeżeniem praw osób trzecich, decyzji administracyjnych, tytułów prawnych do nieruchomości, warunków technicznych zarządców infrastruktury oraz innych ograniczeń formalnoprawnych wynikających z przebiegu trasy przyłącza.

Serwerownia zapasowa oraz łącze teleinformatyczne mają stanowić element architektury odpornościowej systemu RIS. Ich zadaniem jest zapewnienie warunków technicznych do replikacji danych, przechowywania kopii lub replik zasobów systemowych, odtworzenia wybranych funkcji systemu po awarii, ograniczenia skutków niedostępności serwerowni głównej oraz zapewnienia bezpiecznej i kontrolowanej komunikacji pomiędzy lokalizacją podstawową a lokalizacją zapasową.

Utworzenie serwerowni zapasowej nie może być traktowane jako odrębna, niezależna usługa kolokacyjna oderwana od architektury systemu RIS. Rozwiązanie musi zostać zaprojektowane jako część docelowego środowiska teleinformatycznego RIS, powiązana z serwerownią główną, siecią transmisji danych, systemem backupu, pamięcią masową, systemami bezpieczeństwa, monitoringiem technicznym, dokumentacją eksploatacyjną, Planem Ciągłości Działania BCP oraz Planem Odtworzenia po Awarii DRP.

Szczegółowe wymagania dotyczące zewnętrznego Data Center, szafy teleinformatycznej RACK, przyłącza energetycznego, licznika energii, przyłącza światłowodowego 6J, własności infrastruktury, utrzymania, kosztów eksploatacyjnych, SLA, monitoringu, bezpieczeństwa, testów, dokumentacji, gwarancji i przekazania do eksploatacji określono w rozdziale 1.2.13 Wymagania dla ośrodka zapasowego i łącza teleinformatycznego.

1.1.2.12. Usługi cyfrowe RIS

Przedmiot zamówienia obejmuje zaprojektowanie, wykonanie, modernizację, integrację, konfigurację, uruchomienie, przetestowanie i przekazanie do eksploatacji wybranych usług cyfrowych systemu RIS, wspierających pracę Centrum RIS, obsługę danych dziedzinowych systemu RIS, integrację z systemami zewnętrznymi oraz udostępnianie danych uprawnionym odbiorcom.

Usługi cyfrowe realizowane w ramach niniejszego zamówienia mają stanowić część zmodernizowanego systemu RIS i muszą być spójne z docelową architekturą systemu, modelem danych, mechanizmami integracji, zasadami bezpieczeństwa, wymaganiami interoperacyjności, wymaganiami dostępności cyfrowej oraz wymaganiami dotyczącymi utrzymania, monitorowania i rozwoju systemu.

Zakres tej części zamówienia nie obejmuje wykonania aplikacji mapowej stanowiącej podstawowy kanał prezentacji danych przestrzennych i informacji dla użytkowników śródlądowych dróg wodnych. Zamawiający przewiduje realizację aplikacji mapowej w ramach odrębnego zamówienia. W konsekwencji niniejsze zamówienie nie obejmuje również funkcji, które zostaną zrealizowane w tej aplikacji, w szczególności mobilnego albo responsywnego dostępu użytkowników do aplikacji mapowej, obsługi zgłoszeń użytkowników dotyczących drogi wodnej, prezentacji komunikatów NtS w aplikacji mapowej, powiązania aplikacji mapowej z Inland ECDIS, automatycznymi komunikatami NtS, informacją o stanie wody oraz informacją o prześwitach mostowych.

Wyłączenie aplikacji mapowej z zakresu niniejszego zamówienia nie zwalnia Generalnego Wykonawcy z obowiązku zapewnienia, aby zmodernizowany system RIS dostarczał dane, usługi integracyjne, interfejsy oraz mechanizmy udostępniania danych niezbędne do późniejszej integracji z aplikacją mapową Zamawiającego oraz innymi systemami wewnętrznymi lub zewnętrznymi wskazanymi przez Zamawiającego.

W ramach niniejszego zamówienia Generalny Wykonawca zobowiązany jest zapewnić w szczególności cyfrowe usługi i komponenty systemowe związane z pozyskiwaniem, przetwarzaniem, walidacją, korektą, przechowywaniem, archiwizacją, udostępnianiem i wymianą danych dziedzinowych systemu RIS. Dotyczy to w szczególności danych pochodzących z podsystemów VHF/AIS/DGNSS, CCTV w zakresie wymaganych metadanych i statusów

technicznych, czujników hydrologicznych, sensorów meteorologicznych, sieci transmisji danych, lokalizacji terenowych, infrastruktury technicznej oraz systemów monitoringu technicznego.

Istotnym elementem usług cyfrowych realizowanych w ramach niniejszego zamówienia jest zapewnienie mechanizmów udostępniania danych i informacji różnym grupom użytkowników oraz systemom zewnętrznym. Zakres ten obejmuje w szczególności integrację z systemem EuRIS, integrację z Systemem Hydrologii IMGW-PIB oraz wykonanie API systemu RIS służącego do udostępniania danych dziedzinowych systemom własnym Zamawiającego, przyszłej aplikacji mapowej oraz uprawnionym interesariuszom zewnętrznym. Szczegółowe wymagania dotyczące interoperacyjności, modelu danych, integracji z systemami zewnętrznymi oraz API systemu RIS określono w rozdziale 1.2.15 „Wymagania interoperacyjności, danych i integracji z systemami zewnętrznymi”.

Zakres usług cyfrowych musi obejmować również rozwiązania umożliwiające obsługę danych hydrologicznych i meteorologicznych systemu RIS, w tym ich odbiór z lokalizacji terenowych, walidację, oznaczanie jakości, korektę w zakresie przewidzianym przez Zamawiającego, archiwizację, udostępnianie do systemów zewnętrznych oraz wykorzystanie w usługach informacyjnych systemu RIS. Rozwiązania te muszą uwzględniać specyfikę pracy czujników hydrologicznych i sensorów meteorologicznych, w tym możliwość opóźnionego przekazania danych po czasowej utracie łączności z Centrum RIS.

Usługi cyfrowe muszą wspierać zarządzanie danymi i konfiguracją systemu RIS, w szczególności w zakresie identyfikacji lokalizacji, urządzeń, punktów pomiarowych, sensorów, kamer, usług, interfejsów, użytkowników technicznych, słowników, statusów, kodów, alarmów oraz innych danych referencyjnych wymaganych do poprawnego działania systemu i jego integracji z systemami zewnętrznymi.

W zakresie objętym niniejszym zamówieniem Generalny Wykonawca zobowiązany jest również zapewnić mechanizmy administracyjne, operatorskie i utrzymaniowe niezbędne do zarządzania dostarczanymi usługami cyfrowymi, ich konfiguracją, uprawnieniami, logami, monitorowaniem, raportowaniem, obsługą błędów, integracją oraz dokumentacją eksploatacyjną.

Dostarczane usługi cyfrowe muszą zostać wykonane jako rozwiązania bezpieczne, udokumentowane, skalowalne, możliwe do utrzymania i dalszego rozwoju. Muszą one umożliwiać integrację z istniejącymi i przyszłymi komponentami systemu RIS oraz z rozwiązaniami realizowanymi przez Zamawiającego w ramach odrębnych zamówień, w szczególności z aplikacją mapową, która będzie korzystała z danych i usług udostępnianych przez zmodernizowany system RIS.

Generalny Wykonawca zobowiązany jest zapewnić, aby usługi cyfrowe objęte niniejszym zamówieniem były zgodne z wymaganiami dotyczącymi cyberbezpieczeństwa, dostępności cyfrowej, interoperacyjności, jakości danych, ochrony danych, dokumentacji, testów, odbiorów, gwarancji, monitoringu technicznego oraz utrzymania. Wymagania szczegółowe dla usług cyfrowych określono w rozdziale 1.2.14 „Wymagania dla usług cyfrowych”, natomiast wymagania dotyczące integracji, API i udostępniania danych określono w rozdziale 1.2.15 Wymagania interoperacyjności, danych i integracji z systemami zewnętrznymi.

1.1.2.13. Monitoring techniczny zasobów infrastrukturalnych i aplikacyjnych systemu

Przedmiot zamówienia obejmuje zaprojektowanie, wykonanie, rozbudowę, konfigurację, integrację, uruchomienie, przetestowanie i przekazanie do eksploatacji rozwiązań monitoringu technicznego zasobów infrastrukturalnych i aplikacyjnych systemu RIS. Monitoring techniczny ma stanowić wspólną, przekrojową warstwę nadzoru nad dostępnością, stanem pracy, zdarzeniami, alarmami i podstawowymi parametrami eksploatacyjnymi komponentów systemu RIS.

Celem tej części zamówienia jest zapewnienie Zamawiającemu bieżącej wiedzy o stanie technicznym systemu RIS, w tym o stanie urządzeń terenowych, urządzeń sieciowych, urządzeń transmisyjnych, infrastruktury serwerowej, maszyn wirtualnych, usług aplikacyjnych, usług integracyjnych, systemów zasilania, elementów środowiskowych szaf i serwerowni, komponentów CCTV, komponentów VHF/AIS/DGNSS, czujników hydrologicznych, sensorów meteorologicznych oraz innych zasobów mających wpływ na ciągłość działania usług RIS.

Na obszarze aktualnego działania systemu RIS Zamawiający eksploatuje rozwiązania służące do monitorowania zdarzeń, dostępności i stanu pracy wybranych zasobów infrastrukturalnych, sieciowych, środowiskowych oraz aplikacyjnych systemu RIS. Obecny model monitorowania obejmuje w szczególności wykorzystanie systemu NetCrunch do monitorowania dostępności urządzeń sieciowych, serwerów, komputerów, maszyn wirtualnych, przełączników, zasobów serwerowni oraz raportowania dostępności, systemu UISP do monitorowania elementów sieci transmisyjnej i urządzeń radiowych, systemu BKT SM4DC do monitorowania parametrów środowiskowych i zdarzeń w szafach teletechnicznych, systemu ELVYS do monitorowania elementów związanych z łącznością VHF, a także mechanizmów monitorowania stron WWW oraz usług WebServices.

Informacja o aktualnie wykorzystywanych rozwiązaniach monitorowania ma charakter opisu stanu istniejącego oraz punktu odniesienia dla zachowania ciągłości eksploatacyjnej, organizacji utrzymania, sposobu prezentacji zdarzeń, alarmowania, raportowania dostępności oraz włączenia nowych i modernizowanych zasobów systemu RIS do spójnego modelu monitoringu technicznego. Nie oznacza ona obowiązku zastosowania wyłącznie tych samych produktów albo technologii, chyba że jest to niezbędne dla zapewnienia kompatybilności, ciągłości działania, integracji z istniejącym środowiskiem Zamawiającego albo zachowania dotychczasowego sposobu pracy służb technicznych Zamawiającego.

Generalny Wykonawca zobowiązany jest przed zaprojektowaniem docelowego rozwiązania monitoringu technicznego przeanalizować aktualnie eksploatowane przez Zamawiającego narzędzia monitorowania, ich konfigurację, zakres monitorowanych zasobów, sposób grupowania lokalizacji i urządzeń, sposób prezentacji alarmów, progi alarmowe, raporty, integracje, ograniczenia licencyjne oraz możliwości rozbudowy. Wyniki tej analizy muszą zostać wykorzystane przy opracowaniu docelowej koncepcji monitoringu technicznego zasobów infrastrukturalnych i aplikacyjnych systemu RIS.

Zakres tej części zamówienia obejmuje zarówno objęcie monitoringiem technicznym nowych zasobów dostarczanych w ramach projektu, jak również dostosowanie, rozbudowę albo rekonfigurację istniejącego systemu monitorowania zdarzeń wykorzystywanego przez Zamawiającego dla obecnego obszaru działania systemu RIS. Generalny Wykonawca

zobowiązany będzie zapewnić, aby nowe i modernizowane komponenty systemu RIS zostały włączone do spójnego modelu monitorowania, alarmowania, raportowania i obsługi zdarzeń technicznych.

Monitoring techniczny musi obejmować co najmniej następujące grupy zasobów, o ile występują w docelowej architekturze systemu RIS:

1) urządzenia sieciowe i transmisyjne, w tym przełączniki, routery, modemy, urządzenia dostępowe, urządzenia zestawiające tory transmisyjne, urządzenia VPN, zapory sieciowe oraz elementy redundancji transmisji danych;
2) system łączności radiowej VHF/AIS/DGNSS, w tym urządzenia stacji brzegowych, urządzenia nadawczo-odbiorcze, urządzenia systemów antenowych, komponenty aplikacyjne, konsole operatorskie, usługi i elementy odpowiedzialne za nadzór nad stanem pracy warstwy radiokomunikacyjnej;
3) system monitoringu wizyjnego CCTV, w tym kamery obserwacyjne, kamery dozorowe, rejestratory, węzły rejestracji, strumienie wideo, stacje klienckie, usługi udostępniania obrazu, komponenty integracyjne, zdarzenia i alarmy techniczne;
4) czujniki hydrologiczne i sensory meteorologiczne, w tym lokalne komponenty akwizycji danych, sterowniki, konwertery, moduły komunikacyjne, moduły buforowania danych, zasilanie, transmisję danych i status poprawności przekazywania danych pomiarowych;
5) szafy teletechniczne typu zewnętrznego i ich wyposażenie, w tym monitoring parametrów środowiskowych, otwarcia drzwi, kontroli dostępu, zasilania, UPS, listew zasilających, liczników energii, wentylacji, ogrzewania i innych elementów wyposażenia technicznego;
6) elementy infrastruktury energetycznej, w tym zasilacze awaryjne, moduły bateryjne, PDU, agregaty prądotwórcze, zasilanie rezerwowe, elementy monitoringu zasilania i alarmy środowiskowe;
7) infrastrukturę serwerową i wirtualizacyjną, w tym serwery fizyczne, serwery kasetowe, hosty wirtualizacyjne, maszyny wirtualne, zasoby dyskowe, macierze, systemy backupu, elementy replikacji oraz komponenty środowiska serwerowni głównej i zapasowej;
8) usługi aplikacyjne systemu RIS, w tym usługi cyfrowe, aplikacje operatorskie, usługi VTT, usługi informacji hydrometeorologicznej, portale, aplikacje mapowe, interfejsy API, usługi integracyjne oraz usługi WebServices;
9) strony WWW, portale, interfejsy użytkownika i usługi publikacyjne udostępniane przez system RIS;
10) komponenty systemów bezpieczeństwa, kontroli dostępu, logowania zdarzeń oraz inne elementy wymagające monitorowania ze względu na utrzymanie ciągłości działania i bezpieczeństwa systemu RIS.

Monitoring techniczny powinien umożliwiać prezentację stanu zasobów w układzie odpowiadającym strukturze systemu RIS, w szczególności w podziale na lokalizacje terenowe, podsystemy, grupy urządzeń, zasoby centralne, usługi aplikacyjne, usługi integracyjne i środowiska techniczne. Rozwiązanie powinno umożliwiać szybkie ustalenie czy zdarzenie dotyczy pojedynczego urządzenia, lokalizacji terenowej, toru transmisyjnego, usługi aplikacyjnej,

komponentu centralnego, zasilania, środowiska pracy urządzeń albo innego elementu wpływającego na dostępność usług RIS.

Generalny Wykonawca zobowiązany będzie zapewnić, aby monitoring techniczny nowych i modernizowanych zasobów był realizowany w sposób spójny z aktualnym modelem monitorowania systemu RIS oraz dotychczasowym sposobem pracy służb technicznych Zamawiającego. Oznacza to konieczność zachowania albo odtworzenia co najmniej dotychczasowych funkcji monitorowania, a także ich rozszerzenia o nowe zasoby, lokalizacje, urządzenia, usługi aplikacyjne i integracje powstające w ramach projektu.

Generalny Wykonawca zobowiązany będzie zapewnić, aby monitoring techniczny nowych i modernizowanych zasobów był realizowany w sposób spójny z dotychczasowym sposobem pracy służb technicznych Zamawiającego. Oznacza to konieczność zachowania albo odtworzenia co najmniej dotychczasowych funkcji monitorowania, a także ich rozszerzenia o nowe zasoby i usługi powstające w ramach projektu.

Zakres tej części zamówienia obejmuje w szczególności:

1) analizę obecnego systemu monitorowania zdarzeń oraz sposobu jego wykorzystania przez Zamawiającego;
2) opracowanie docelowej koncepcji monitoringu technicznego zasobów infrastrukturalnych i aplikacyjnych systemu RIS;
3) objęcie monitoringiem technicznym wszystkich nowych i modernizowanych zasobów systemu RIS, które mają wpływ na dostępność, bezpieczeństwo, transmisję danych, rejestrację danych, świadczenie usług cyfrowych albo utrzymanie lokalizacji terenowych;
4) konfigurację monitorowania dostępności urządzeń i usług;
5) konfigurację monitorowania parametrów pracy urządzeń, jeżeli urządzenia udostępniają takie dane;
6) konfigurację alarmów, progów alarmowych, statusów, zdarzeń, powiadomień i klasyfikacji zdarzeń technicznych;
7) konfigurację widoków lokalizacyjnych, widoków podsystemów, widoków centralnych i widoków usług aplikacyjnych;
8) integrację monitoringu z systemem zarządzania i utrzymania zasobów RIS;
9) zapewnienie raportowania dostępności zasobów, podsystemów, usług i lokalizacji;
10) wykonanie testów poprawności monitorowania, alarmowania i raportowania;
11) przygotowanie dokumentacji powykonawczej, konfiguracyjnej, eksploatacyjnej i administracyjnej monitoringu technicznego;
12) przeszkolenie wskazanych użytkowników Zamawiającego w zakresie obsługi, administracji i interpretacji zdarzeń monitoringu technicznego.

Monitoring techniczny musi wspierać utrzymanie ciągłości działania systemu RIS, w szczególności poprzez wczesną identyfikację awarii, degradacji jakości pracy, utraty komunikacji, utraty zasilania, przekroczenia dopuszczalnych parametrów środowiskowych,

błędów usług aplikacyjnych, niedostępności interfejsów, błędów integracji, utraty strumieni wideo, utraty danych pomiarowych albo innych zdarzeń mogących wpływać na pracę Centrum RIS, aplikacji operatorskich, usług cyfrowych, infrastruktury terenowej lub systemów zewnętrznych.

W odniesieniu do lokalizacji terenowych monitoring techniczny powinien umożliwiać nadzór nad stanem lokalizacji jako kompletnego punktu infrastruktury RIS. Obejmuje to w szczególności możliwość monitorowania stanu urządzeń aktywnych, transmisji danych, zasilania, UPS, urządzeń pomiarowych, kamer, urządzeń radiokomunikacyjnych, elementów szafy teletechnicznej, parametrów środowiskowych, kontroli dostępu oraz dostępności usług realizowanych przez daną lokalizację.

W odniesieniu do zasobów centralnych monitoring techniczny powinien obejmować co najmniej infrastrukturę serwerową, środowisko wirtualizacyjne, maszyny wirtualne, przełączniki, zapory sieciowe, systemy przechowywania danych, systemy rejestracji i archiwizacji, systemy backupu, usługi aplikacyjne, usługi integracyjne, portale, API, WebServices oraz elementy środowiska serwerowni wpływające na ciągłość działania systemu RIS.

W odniesieniu do podsystemu CCTV monitoring techniczny powinien obejmować co najmniej stan kamer, rejestratorów, węzłów rejestracji, stacji klienckich, strumieni wideo, usług udostępniania obrazu, komponentów integracyjnych, funkcji zdarzeń i alarmów oraz elementów wpływających na ciągłość rejestracji, podglądu, odtwarzania i eksportu materiału wideo.

W odniesieniu do podsystemu VHF/AIS/DGNSS monitoring techniczny powinien obejmować co najmniej stan urządzeń stacji brzegowych, komponentów aplikacyjnych, urządzeń komunikacyjnych, usług i konsol prezentujących stan systemu radiokomunikacyjnego, a także zdarzenia wpływające na dostępność łączności głosowej VHF, odbiór i przetwarzanie danych AIS oraz funkcje DGNSS.

W odniesieniu do czujników hydrologicznych i sensorów meteorologicznych monitoring techniczny powinien obejmować nie tylko dostępność komunikacyjną urządzeń, lecz również stan lokalnych komponentów odpowiedzialnych za pozyskiwanie, buforowanie, przetwarzanie i przekazywanie danych pomiarowych do Centrum RIS. Monitoring powinien umożliwiać identyfikację przerwy w komunikacji, błędów urządzenia, braku nowych danych, opóźnienia w przekazaniu danych, utraty zasilania lub innych zdarzeń wpływających na wiarygodność i ciągłość danych pomiarowych.

W ramach monitoringu technicznego Generalny Wykonawca zobowiązany będzie zapewnić możliwość raportowania dostępności zasobów i usług systemu RIS. Raportowanie powinno umożliwiać analizę dostępności poszczególnych komponentów, lokalizacji, usług, podsystemów i całego systemu RIS w zadanym okresie, w szczególności na potrzeby utrzymania, gwarancji, obsługi awarii, analizy przyczyn problemów oraz weryfikacji poziomu dostępności usług.

Rozwiązanie monitoringu technicznego musi zostać wykonane w sposób umożliwiający jego dalszą rozbudowę. Dotyczy to w szczególności możliwości dodawania kolejnych lokalizacji, urządzeń, usług, interfejsów, sensorów, kamer, elementów transmisyjnych, maszyn wirtualnych, komponentów aplikacyjnych i usług cyfrowych bez konieczności przebudowy całej architektury monitoringu.

Realizacja tej części zamówienia obejmuje również dostarczenie wszystkich licencji, subskrypcji, modułów, konektorów, agentów, uprawnień technicznych, szablonów monitorowania, profili

urządzeń oraz innych komponentów wymaganych do objęcia monitoringiem zasobów dostarczanych, modernizowanych, rekonfigurowanych albo integrowanych przez Generalnego Wykonawcę. Brak licencji, modułu, agenta, konektora albo innego uprawnienia technicznego nie może ograniczać możliwości monitorowania zasobów objętych przedmiotem zamówienia.

Generalny Wykonawca zobowiązany będzie przekazać Zamawiającemu kompletną dokumentację monitoringu technicznego, obejmującą co najmniej wykaz monitorowanych zasobów, sposób ich identyfikacji, adresację, nazewnictwo, przypisanie do lokalizacji i podsystemów, zakres monitorowanych parametrów, progi alarmowe, reguły alarmowania, sposób powiadamiania, zasady raportowania, procedury eksploatacyjne, procedury aktualizacji konfiguracji oraz instrukcje dla administratorów i użytkowników utrzymaniowych.

Szczegółowe wymagania dotyczące zakresu monitoringu technicznego, monitorowanych parametrów, progów alarmowych, powiadomień, integracji, raportowania, dokumentacji, testów, odbioru, gwarancji i utrzymania zostaną określone w dalszych rozdziałach PFU oraz w dokumentacji projektowej opracowanej przez Generalnego Wykonawcę

1.2. Opis wymagań Zamawiającego w stosunku do przedmiotu zamówienia

Rozdział określa wymagania Zamawiającego w stosunku do przedmiotu zamówienia realizowanego w formule „zaprojektuj i zbuduj”. Wymagania te stanowią podstawę do opracowania przez Generalnego Wykonawcę dokumentacji projektowej, doboru rozwiązań technicznych, wykonania robót, dostaw, instalacji, konfiguracji, integracji, testów, odbiorów, dokumentacji powykonawczej, przekazania systemu do eksploatacji oraz świadczenia gwarancji, serwisu i usług utrzymaniowych.

Wymagania określone w niniejszym rozdziale obejmują zarówno wymagania przekrojowe, mające zastosowanie do całości przedmiotu zamówienia, jak również wymagania szczegółowe dotyczące poszczególnych podsystemów, komponentów, usług, instalacji, robót i dokumentów. Obejmują one w szczególności zgodność prawną i normatywną, zasady projektowania, system łączności radiowej VHF/AIS/DGNSS, system monitoringu wizyjnego CCTV, sieć połączeń transmisyjnych, czujniki hydrologiczne i meteorologiczne, infrastrukturę terenową, zasilanie awaryjne, serwerownie, sieć teleinformatyczną, środowisko pracy systemu RIS, usługi cyfrowe, interoperacyjność, dostępność cyfrową, cyberbezpieczeństwo, dokumentację, procedury testowania i odbioru, szkolenia, przekazanie do eksploatacji, gwarancję, serwis, przeglądy techniczne i Usługę Utrzymania.

Wymagania wskazane w niniejszym rozdziale należy interpretować łącznie z opisem ogólnym przedmiotu zamówienia, dokumentami branżowymi stanowiącymi załączniki do PFU, dokumentacją informacyjną, obowiązującymi przepisami prawa, normami, standardami technicznymi, wymaganiami producentów oraz postanowieniami Umowy. W przypadku gdy wymaganie szczegółowe odnoszące się do danego podsystemu, lokalizacji, urządzenia albo usługi doprecyzowuje wymaganie ogólne, Generalny Wykonawca zobowiązany jest spełnić oba wymagania w sposób zapewniający kompletność, spójność, bezpieczeństwo, interoperacyjność i gotowość eksploatacyjną całego systemu RIS.

Generalny Wykonawca zobowiązany jest traktować wymagania niniejszego rozdziału jako minimalny zakres odpowiedzialności technicznej, organizacyjnej, projektowej, wykonawczej, integracyjnej, dokumentacyjnej i utrzymaniowej. Brak wyszczególnienia w PFU pojedynczego elementu, czynności, materiału, licencji, konfiguracji, interfejsu, testu albo dokumentu nie zwalnia Generalnego Wykonawcy z obowiązku jego zapewnienia, jeżeli jest on niezbędny do prawidłowego zaprojektowania, wykonania, uruchomienia, zintegrowania, przetestowania, utrzymania albo bezpiecznej eksploatacji systemu RIS.

1.2.1. Wymagania w stosunku do zgodności prawnej i normatywnej

Wymagania określone w niniejszym rozdziale wyznaczają podstawowy reżim prawny, normatywny i techniczny, w którym Generalny Wykonawca zobowiązany jest zaprojektować, wykonać, dostarczyć, zintegrować, przetestować, udokumentować i przekazać do eksploatacji przedmiot zamówienia.

Rozbudowa systemu RIS na Odrzańskiej Drodze Wodnej jest przedsięwzięciem wielobranżowym, obejmującym równocześnie elementy infrastruktury teleinformatycznej, radiokomunikacyjnej, obserwacyjnej, sensorowej, serwerowej, aplikacyjnej, transmisyjnej, budowlanej, energetycznej i środowiskowej. Z tego względu realizacja zamówienia wymaga zapewnienia zgodności nie tylko z przepisami bezpośrednio dotyczącymi usług informacji rzecznej RIS i żeglugi śródlądowej, lecz również z przepisami oraz normami dotyczącymi zamówień publicznych, dokumentacji projektowej, robót budowlanych, lokalizacji infrastruktury, gospodarki wodnej, ochrony środowiska, łączności elektronicznej, radiokomunikacji, kompatybilności elektromagnetycznej, cyberbezpieczeństwa, ochrony danych, dostępności cyfrowej, interoperacyjności, finansowania ze środków Unii Europejskiej oraz oznakowania projektu.

Wymagania wskazane w niniejszym rozdziale mają charakter przekrojowy i obowiązują dla wszystkich części przedmiotu zamówienia, niezależnie od tego, czy dotyczą one infrastruktury terenowej, komponentów centralnych, usług cyfrowych, sieci transmisyjnej, systemów bezpieczeństwa, oprogramowania, dokumentacji, testów, odbiorów czy późniejszego przekazania systemu do eksploatacji. Generalny Wykonawca zobowiązany jest uwzględniać je na każdym etapie realizacji zamówienia, w szczególności na etapie analiz przedprojektowych, opracowania dokumentacji projektowej, uzyskiwania decyzji, pozwoleń, zgód i uzgodnień, doboru technologii i urządzeń, realizacji robót, konfiguracji systemów, integracji, testowania, odbiorów oraz przygotowania dokumentacji powykonawczej i eksploatacyjnej.

Wymagania prawne i normatywne należy stosować łącznie z wymaganiami funkcjonalnymi, technicznymi, jakościowymi, bezpieczeństwa i eksploatacyjnymi określonymi w pozostałych częściach PFU oraz w załącznikach branżowych, w szczególności w planach dotyczących systemu monitoringu wizyjnego CCTV, łączności radiowej VHF/AIS oraz połączeń transmisyjnych. W przypadku rozbieżności, wątpliwości interpretacyjnych albo zmiany przepisów lub norm w toku realizacji zamówienia Generalny Wykonawca zobowiązany jest do zastosowania rozwiązania zapewniającego zgodność z aktualnie obowiązującym stanem prawnym, wymaganiami Zamawiającego, zasadami bezpieczeństwa, interoperacyjności, trwałości, dostępności i należytej staranności zawodowej.

Niewskazanie w PFU konkretnego aktu prawnego, normy, standardu, wytycznej, decyzji administracyjnej, warunku technicznego albo dokumentu odniesienia nie zwalnia Generalnego Wykonawcy z obowiązku jego zastosowania, jeżeli ma on zastosowanie do projektowanych, dostarczanych, instalowanych, integrowanych, testowanych albo przekazywanych do eksploatacji elementów przedmiotu zamówienia. Generalny Wykonawca ponosi odpowiedzialność za bieżącą identyfikację właściwych podstaw prawnych i normatywnych oraz za wykazanie ich zastosowania w dokumentacji projektowej, wykonawczej, powykonawczej, odbiorowej i eksploatacyjnej.

Spełnienie wymagań prawnych i normatywnych musi zostać potwierdzone odpowiednimi dokumentami, w szczególności deklaracjami zgodności, certyfikatami, atestami, dokumentami dopuszczającymi, protokołami badań i pomiarów, protokołami testów, wynikami odbiorów branżowych, dokumentacją materiałową, dokumentacją konfiguracyjną, dokumentacją bezpieczeństwa, dokumentacją powykonawczą oraz oświadczeniami wymaganymi dla danej kategorii urządzeń, robót, usług, systemów lub oprogramowania. Kompletność tych dokumentów stanowi jeden z warunków potwierdzenia zgodności przedmiotu zamówienia z wymaganiami PFU oraz przekazania systemu RIS do eksploatacji.

1.2.1.1. Klauzula ogólna zgodności prawnej i normatywnej

1) Generalny Wykonawca zrealizuje całość przedmiotu zamówienia zgodnie z obowiązującymi przepisami prawa Unii Europejskiej, przepisami prawa krajowego, aktami wykonawczymi, decyzjami administracyjnymi, warunkami technicznymi, normami, standardami branżowymi oraz dokumentami programowymi właściwymi dla finansowania projektu ze środków Unii Europejskiej wskazanymi w rozdziale Błąd! Nie można odnaleźć źródła odwołania. **Przepisy prawne, normy i standardy związane z projektowanie i wykonaniem zamierzenia inwestycyjnego.**
2) Dla projektowania, dostaw, robót budowlanych, instalacji, konfiguracji, wdrożenia, testów, odbiorów i przekazania do eksploatacji stosuje się akty prawne oraz normy w brzmieniu obowiązującym w dacie wykonywania danej czynności. Jeżeli po sporządzeniu PFU nastąpi zmiana przepisu, publikatora, normy albo standardu, Generalny Wykonawca zastosuje brzmienie aktualne, chyba że bezwzględnie obowiązujące przepisy przejściowe wymagają zastosowania innego reżimu.
3) Jeżeli norma wskazana w PFU została wycofana, zastąpiona albo zmieniona, Generalny Wykonawca zastosuje normę zastępującą, wydanie aktualne albo rozwiązanie równoważne zapewniające nie niższy poziom bezpieczeństwa, funkcjonalności, interoperacyjności, cyberbezpieczeństwa, jakości i trwałości.
4) Niewyszczególnienie w PFU aktu prawnego, normy albo standardu, który ma zastosowanie do zakresu prac, dostaw, usług, robót albo dokumentacji, nie zwalnia Generalnego Wykonawcy z obowiązku jego zastosowania.
5) W razie rozbieżności pomiędzy wymaganiami prawnymi, normatywnymi, technicznymi i funkcjonalnymi Generalny Wykonawca zastosuje wymaganie dalej idące, bardziej rygorystyczne oraz zapewniające wyższy poziom bezpieczeństwa żeglugi, bezpieczeństwa użytkowników, niezawodności systemu RIS, ochrony danych, cyberbezpieczeństwa i trwałości infrastruktury.

6) Każdy komponent systemu RIS, każda dokumentacja projektowa i powykonawcza, każdy element infrastruktury budowlanej, radiowej, teleinformatycznej, serwerowej, zasilającej, monitoringu wizyjnego oraz każda usługa cyfrowa muszą posiadać udokumentowaną zgodność z właściwymi przepisami, normami i standardami. Wymaga się, aby potwierdzenie zgodności było możliwe do zweryfikowania na etapie odbiorów częściowych, odbiorów końcowych oraz przekazania systemu do eksploatacji.

1.2.1.2. Wymagania wynikające z prawa Unii Europejskiej i standardów RIS

1) System RIS po rozbudowie musi spełniać wymagania Dyrektywy 2005/44/WE Parlamentu Europejskiego i Rady z dnia 7 września 2005 r. w sprawie zharmonizowanych usług informacji rzecznej na śródlądowych drogach wodnych we Wspólnocie, w jej aktualnym brzmieniu. Wymaganie obejmuje zapewnienie harmonizacji, interoperacyjności, otwartości, dostępności danych nawigacyjnych, danych do planowania podróży, komunikatów dla kierowników statków, elektronicznych map nawigacyjnych, elektronicznego raportowania oraz wymiany informacji z właściwymi systemami krajowymi i europejskimi.
2) Dla usług informacji rzecznej stosuje się najnowszą edycję Europejskiego Standardu Usług Informacji Rzecznej ES-RIS, przyjętą przez CESNI. Na dzień sporządzenia niniejszego wsadu właściwym odniesieniem jest ES-RIS Edition 2025/1. Zakres zgodności obejmuje w szczególności Inland ECDIS, Vessel Tracking and Tracing, Inland AIS, Notices to Skippers, Electronic Ship Reporting, RIS Index, dane referencyjne, interfejsy wymiany danych oraz wymagania interoperacyjności europejskiego środowiska RIS.
3) Generalny Wykonawca zapewni zgodność projektowanych i wdrażanych usług RIS z Rozporządzeniem Komisji (WE) nr 414/2007 z dnia 13 marca 2007 r. w sprawie wytycznych technicznych dotyczących planowania, wdrażania i wykorzystania operacyjnego usług informacji rzecznej, w zakresie pozostającym w mocy i mającym zastosowanie do projektu.
4) Dla funkcji śledzenia i namierzania statków oraz warstwy Inland AIS stosuje się Rozporządzenie wykonawcze Komisji (UE) 2019/838 z dnia 20 lutego 2019 r. w sprawie specyfikacji technicznych systemów śledzenia i namierzania statków oraz uchylające rozporządzenie (WE) nr 415/2007. Wymaganie obejmuje także właściwe zastosowanie standardów AIS, komunikatów aplikacyjnych, zasad pracy stacji brzegowych, urządzeń wspomagających nawigację i wymiany danych VTT.
5) Dla elektronicznego raportowania statków stosuje się Rozporządzenie wykonawcze Komisji (UE) 2019/1744 z dnia 17 września 2019 r. w sprawie specyfikacji technicznych elektronicznego raportowania statków w żegludze śródlądowej oraz uchylające rozporządzenie (UE) nr 164/2010. Wymaganie obejmuje komunikaty, dane, słowniki, kody, identyfikatory, reguły walidacji i interfejsy wymiany danych wymagane dla ERI.
6) Dla komunikatów dla kierowników statków stosuje się obowiązujące przepisy wykonawcze i standardy techniczne wydane na podstawie Dyrektywy 2005/44/WE oraz aktualny ES-RIS. Wymaganie obejmuje generowanie, odbiór, przetwarzanie, dystrybucję

i archiwizację komunikatów w sposób ustandaryzowany, kodowany, aktualny, dostępny i możliwy do wymiany z innymi środowiskami RIS.

7) Dla elektronicznych map nawigacyjnych śródlądowych stosuje się obowiązujące przepisy wykonawcze i standardy techniczne Inland ECDIS, aktualny ES-RIS oraz właściwe specyfikacje danych Inland ENC. Wymaganie obejmuje zgodność danych przestrzennych, symbolizacji, atrybutów, sposobu dystrybucji, walidacji, aktualizacji i wykorzystania map w usługach RIS.

8) W zakresie technicznych wymagań dla statków żeglugi śródlądowej, jeżeli wymagania te wpływają na interfejsy, dane, komunikację albo kompatybilność systemu RIS z użytkownikami śródlądowych dróg wodnych, stosuje się Dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1629 z dnia 14 września 2016 r. ustanawiającą wymagania techniczne dla statków żeglugi śródlądowej i uchylającą dyrektywę 2006/87/WE, wraz z aktami zmieniającymi i wykonawczymi.

9) W zakresie interoperacyjności sektora publicznego stosuje się Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/903 z dnia 13 marca 2024 r. w sprawie ustanowienia środków na rzecz wysokiego poziomu interoperacyjności sektora publicznego na terytorium Unii. Wymaganie obejmuje projektowanie usług cyfrowych RIS, interfejsów, modeli danych, API, wymiany danych oraz dokumentacji technicznej w sposób wspierający interoperacyjność transgraniczną, techniczną, semantyczną, organizacyjną i prawną.

10) W zakresie identyfikacji elektronicznej, usług zaufania, podpisów, pieczęci, znaczników czasu i uwierzytelnienia, jeżeli zostaną zastosowane w systemie RIS, stosuje się Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 eIDAS, w brzmieniu zmienionym Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2024/1183.

11) W zakresie produktów z elementami cyfrowymi stosuje się Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 w sprawie horyzontalnych wymagań cyberbezpieczeństwa dla produktów z elementami cyfrowymi, w zakresie i terminach jego stosowania. Wymaganie obejmuje produkty sprzętowe i programowe dostarczane w ramach systemu RIS, o ile mieszczą się w zakresie tego rozporządzenia.

12) Jeżeli w ramach systemu CCTV, usług cyfrowych RIS, analityki ruchu, statystyk albo automatycznego wspomagania decyzji zostaną zastosowane funkcje oparte na sztucznej inteligencji, Generalny Wykonawca zapewni zgodność z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2024/1689 w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji, w zakresie właściwym dla klasyfikacji i sposobu wykorzystania danego systemu AI.

1.2.1.3. Wymagania wynikające z polskich przepisów dotyczących RIS, żeglugi śródlądowej i dróg wodnych

1) Generalny Wykonawca zastosuje ustawę z dnia 21 grudnia 2000 r. o żegludze śródlądowej, w aktualnym tekście jednolitym Dz.U. 2025 poz. 18 z późniejszymi zmianami. Wymaganie obejmuje w szczególności przepisy dotyczące prowadzenia zharmonizowanego systemu usług informacji rzecznej, właściwości organów żeglugi

śródlądowej, zasad funkcjonowania usług RIS oraz danych i rejestrów wykorzystywanych w żegludze śródlądowej.

2) W zakresie udostępniania danych niezbędnych do funkcjonowania systemu RIS stosuje się Rozporządzenie Ministra Infrastruktury z dnia 14 maja 2026 r. w sprawie udostępniania danych niezbędnych do funkcjonowania systemu usług informacji rzecznej, Dz.U. 2026 poz. 674. Wymaganie obejmuje zakres, rodzaj, częstotliwość i sposób przekazywania danych do właściwego dyrektora urzędu żeglugi śródlądowej oraz techniczne przygotowanie systemu do przyjmowania, przetwarzania i udostępniania tych danych.

3) W zakresie wykazu śródlądowych dróg wodnych, na których wprowadza się usługi informacji rzecznej, stosuje się Rozporządzenie Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 8 stycznia 2013 r., Dz.U. 2013 poz. 80, z późniejszymi zmianami, w szczególności zmianą ogłoszoną w Dz.U. 2024 poz. 1711.

4) W zakresie klasyfikacji śródlądowych dróg wodnych stosuje się Rozporządzenie Rady Ministrów z dnia 7 maja 2002 r. w sprawie klasyfikacji śródlądowych dróg wodnych, Dz.U. 2022 poz. 1170 z późniejszymi zmianami, w tym zmianą ogłoszoną w Dz.U. 2026 poz. 28. Wymaganie obejmuje prawidłowe przypisanie klasy drogi wodnej, analizę ograniczeń nawigacyjnych oraz uwzględnienie parametrów drogi wodnej w projektowaniu lokalizacji i funkcji systemu RIS.

5) W zakresie wykazu śródlądowych dróg wodnych stosuje się Rozporządzenie Rady Ministrów z dnia 26 czerwca 2019 r. w sprawie śródlądowych dróg wodnych, Dz.U. 2019 poz. 1208 z późniejszymi zmianami, w tym zmianą ogłoszoną w Dz.U. 2026 poz. 29, w zakresie, w jakim akt ten identyfikuje odcinki wód istotne dla projektowania i eksploatacji systemu RIS.

6) W zakresie korzystania z wód, lokalizacji infrastruktury na obiektach hydrotechnicznych, w pasach technicznych, na terenach zarządzanych przez PGW Wody Polskie, w pobliżu urządzeń wodnych oraz w obszarach szczególnego zagrożenia powodzią stosuje się ustawę z dnia 20 lipca 2017 r. – Prawo wodne, Dz.U. 2025 poz. 960 z późniejszymi zmianami, wraz z aktami wykonawczymi.

7) W zakresie żeglugi i współpracy na wodach granicznych stosuje się umowę między Rządem Rzeczypospolitej Polskiej i Rządem Republiki Federalnej Niemiec o żegludze śródlądowej z dnia 8 listopada 1991 r., umowę między Rzecząpospolitą Polską a Republiką Federalną Niemiec o współpracy w dziedzinie gospodarki wodnej na wodach granicznych z dnia 19 maja 1992 r. oraz inne obowiązujące akty i uzgodnienia międzynarodowe właściwe dla granicznego odcinka Odry.

8) W zakresie ochrony wód Odry i wymiany informacji związanej ze stanem wód uwzględnia się umowę w sprawie Międzynarodowej Komisji Ochrony Odry przed Zanieczyszczeniem, sporządzoną we Wrocławiu dnia 11 kwietnia 1996 r., w zakresie mającym znaczenie dla danych hydrologicznych, środowiskowych i eksploatacyjnych systemu RIS.

1.2.1.4. Wymagania dotyczące zamówień publicznych, dokumentacji projektowej

1) Całość dokumentacji, dostaw, robót, usług i odbiorów realizuje się z uwzględnieniem ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych, Dz.U. 2026 poz. 793,

w zakresie odnoszącym się do opisu przedmiotu zamówienia, równoważności rozwiązań, dokumentów przedmiotowych, podwykonawstwa, zmian umowy, kontroli jakości, odbiorów i dowodów zgodności.

2) Dokumentacja projektowa i specyfikacje techniczne wykonania i odbioru robót budowlanych muszą spełniać Rozporządzenie Ministra Rozwoju i Technologii z dnia 20 grudnia 2021 r. w sprawie szczegółowego zakresu i formy dokumentacji projektowej, specyfikacji technicznych wykonania i odbioru robót budowlanych oraz programu funkcjonalno-użytkowego, Dz.U. 2021 poz. 2454.
3) W zakresie stosunków cywilnoprawnych, odpowiedzialności kontraktowej, rękojmi, gwarancji, należytego wykonania zobowiązań oraz przeniesienia praw do dokumentacji i oprogramowania stosuje się ustawę z dnia 23 kwietnia 1964 r. – Kodeks cywilny, tj. Dz.U. 2025 poz. 1071 z późniejszymi zmianami.
4) W dokumentacji projektowej, wykonawczej, powykonawczej, odbiorowej i eksploatacyjnej Generalny Wykonawca wykaże zgodność z wymaganiami prawnymi i normatywnymi poprzez opisy techniczne, zestawienia zgodności, deklaracje, certyfikaty, protokoły badań, protokoły testów, wyniki pomiarów, uzyskane decyzje i pozwolenia oraz dokumenty potwierdzające dopuszczenie wyrobów, urządzeń i oprogramowania do stosowania.

1.2.1.5. Wymagania budowlane, lokalizacyjne i infrastrukturalne

1) Dla projektowania, budowy, przebudowy, montażu, rozbiórki, utrzymania i przekazania do użytkowania obiektów budowlanych oraz urządzeń budowlanych stosuje się ustawę z dnia 7 lipca 1994 r. – Prawo budowlane, Dz.U. 2026 poz. 524, wraz z aktami wykonawczymi. Wymaganie obejmuje m.in. obowiązki uczestników procesu budowlanego, projekt budowlany i techniczny, pozwolenia, zgłoszenia, dziennik budowy, geodezyjną inwentaryzację powykonawczą, nadzór, kontrole, odbiory i zasady użytkowania obiektów.
2) Dla pomieszczeń, budynków i elementów infrastruktury budowlanej stosuje się Rozporządzenie Ministra Infrastruktury z dnia 12 kwietnia 2002 r. w sprawie warunków technicznych, jakim odpowiadają budynki i ich usytuowanie, Dz.U. 2022 poz. 1225 z późniejszymi zmianami. Wymaganie obejmuje bezpieczeństwo konstrukcji, bezpieczeństwo pożarowe, warunki użytkowe, dostępność, instalacje, wymagania środowiskowe oraz wymagania dla pomieszczeń technicznych i serwerowych w zakresie właściwym dla ich funkcji.
3) Dla telekomunikacyjnych obiektów budowlanych stosuje się Rozporządzenie Ministra Cyfryzacji z dnia 26 maja 2023 r. w sprawie warunków technicznych, jakim odpowiadają telekomunikacyjne obiekty budowlane i ich usytuowanie, Dz.U. 2023 poz. 1040. Wymaganie obejmuje projektowanie, posadowienie, bezpieczeństwo, konstrukcje wsporcze, instalacje, uziemienie, ochronę odgromową, zabezpieczenia, dostęp eksploatacyjny i usytuowanie obiektów telekomunikacyjnych.
4) Dla kanałów technologicznych stosuje się Rozporządzenie Ministra Cyfryzacji z dnia 26 maja 2023 r. w sprawie warunków technicznych, jakim odpowiadają kanały technologiczne i ich usytuowanie, Dz.U. 2023 poz. 1039. Wymaganie obejmuje budowę,

przebudowę i wykorzystanie kanałów technologicznych dla kabli telekomunikacyjnych, energetycznych i światłowodowych w zakresie dopuszczonym prawem i wymaganym projektem.

5) Dla lokalizacji infrastruktury w przestrzeni, na działkach, obiektach mostowych, obiektach hydrotechnicznych, terenach kolejowych, pasach drogowych i terenach objętych planowaniem przestrzennym stosuje się ustawę z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym, Dz.U. 2026 poz. 538, wraz z aktami wykonawczymi i dokumentami planistycznymi właściwymi dla danej lokalizacji.
6) Dla prac geodezyjnych, map do celów projektowych, wyznaczania lokalizacji, inwentaryzacji powykonawczej, dokumentacji kartograficznej i danych przestrzennych stosuje się ustawę z dnia 17 maja 1989 r. – Prawo geodezyjne i kartograficzne, Dz.U. 2024 poz. 1151 z późniejszymi zmianami, wraz z aktami wykonawczymi.
7) Dla prac prowadzonych w pasach drogowych, na drogowych obiektach inżynierskich, w obrębie mostów, dojazdów i urządzeń drogi stosuje się ustawę z dnia 21 marca 1985 r. o drogach publicznych, Dz.U. 2025 poz. 889 z późniejszymi zmianami, a także przepisy techniczno-budowlane dotyczące dróg publicznych i drogowych obiektów inżynierskich.
8) Dla prac na obiektach kolejowych, w obszarach kolejowych i w sąsiedztwie linii kolejowych stosuje się ustawę z dnia 28 marca 2003 r. o transporcie kolejowym oraz właściwe akty wykonawcze, wymagania zarządców infrastruktury i przepisy bezpieczeństwa obowiązujące dla infrastruktury kolejowej.
9) Dla obiektów zabytkowych, obszarów objętych ochroną konserwatorską, stanowisk archeologicznych i prac mogących wpływać na zabytki stosuje się ustawę z dnia 23 lipca 2003 r. o ochronie zabytków i opiece nad zabytkami, Dz.U. 2024 poz. 1292 z późniejszymi zmianami.
10) Dla ochrony przeciwpożarowej obiektów, pomieszczeń technicznych, serwerowni, zasilania, tras kablowych, szaf, urządzeń i przestrzeni instalacyjnych stosuje się ustawę z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej oraz Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 7 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów, Dz.U. 2023 poz. 822 z późniejszymi zmianami.
11) Dla wyrobów budowlanych stosuje się Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 305/2011 ustanawiające zharmonizowane warunki wprowadzania do obrotu wyrobów budowlanych oraz ustawę z dnia 16 kwietnia 2004 r. o wyrobach budowlanych, Dz.U. 2021 poz. 1213 z późniejszymi zmianami. Wymaganie obejmuje stosowanie wyrobów posiadających właściwe deklaracje właściwości użytkowych, oznakowanie CE albo znak budowlany oraz dokumenty dopuszczające do zastosowania.
12) Dla przyłączy, zasilania podstawowego, zasilania rezerwowego, układów pomiarowych i współpracy z operatorami systemów dystrybucyjnych stosuje się ustawę z dnia 10 kwietnia 1997 r. – Prawo energetyczne, Dz.U. 2026 poz. 43 z późniejszymi zmianami, wraz z aktami wykonawczymi, instrukcjami ruchu i eksploatacji sieci dystrybucyjnych oraz warunkami przyłączenia.

1.2.1.6. Wymagania środowiskowe, wodnoprawne, odpadowe i PEM

1) Dla oceny oddziaływania przedsięwzięcia na środowisko, kwalifikacji przedsięwzięcia, decyzji o środowiskowych uwarunkowaniach, analiz wariantowych, obszarów Natura 2000 i uzgodnień środowiskowych stosuje się ustawę z dnia 3 października 2008 r. o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko, Dz.U. 2024 poz. 1112 z późniejszymi zmianami.
2) Dla ochrony środowiska, emisji, hałasu, pól elektromagnetycznych, obowiązków pomiarowych i korzystania ze środowiska stosuje się ustawę z dnia 27 kwietnia 2001 r. – Prawo ochrony środowiska, Dz.U. 2025 poz. 647 z późniejszymi zmianami.
3) Dla ochrony przyrody, obszarów chronionych, gatunków chronionych, drzew, krzewów, siedlisk, korytarzy ekologicznych i obszarów Natura 2000 stosuje się ustawę z dnia 16 kwietnia 2004 r. o ochronie przyrody, Dz.U. 2026 poz. 13 z późniejszymi zmianami.
4) Dla robót i instalacji mogących wymagać zgód wodnoprawnych, zgłoszeń wodnoprawnych, pozwoleń wodnoprawnych, uzgodnień z właścicielem wód albo zarządcą urządzeń wodnych stosuje się ustawę z dnia 20 lipca 2017 r. – Prawo wodne, Dz.U. 2025 poz. 960 z późniejszymi zmianami.
5) Dla gospodarki odpadami powstającymi podczas budowy, demontażu, modernizacji i eksploatacji stosuje się ustawę z dnia 14 grudnia 2012 r. o odpadach, Dz.U. 2023 poz. 1587 z późniejszymi zmianami. Wymaganie obejmuje klasyfikację odpadów, magazynowanie, transport, przekazanie uprawnionym podmiotom, ewidencję i zagospodarowanie zgodnie z hierarchią postępowania z odpadami.
6) Dla sprzętu elektrycznego i elektronicznego stosuje się ustawę z dnia 11 września 2015 r. o zużytym sprzęcie elektrycznym i elektronicznym, Dz.U. 2024 poz. 573 z późniejszymi zmianami. Wymaganie obejmuje legalne zagospodarowanie demontowanych urządzeń, elementów ICT, kamer, urządzeń zasilających, sprzętu sieciowego, serwerów, pamięci masowych i osprzętu.
7) Dla baterii, akumulatorów, modułów bateryjnych UPS i elementów zasilania awaryjnego stosuje się ustawę z dnia 24 kwietnia 2009 r. o bateriach i akumulatorach, Dz.U. 2025 poz. 809 z późniejszymi zmianami, a także właściwe przepisy unijne dotyczące baterii, w zakresie mającym zastosowanie do dostaw, eksploatacji i zagospodarowania odpadów.
8) Dla opakowań i odpadów opakowaniowych stosuje się ustawę z dnia 13 czerwca 2013 r. o gospodarce opakowaniami i odpadami opakowaniowymi, Dz.U. 2025 poz. 870 z późniejszymi zmianami.
9) Dla pól elektromagnetycznych stosuje się Rozporządzenie Ministra Zdrowia z dnia 17 grudnia 2019 r. w sprawie dopuszczalnych poziomów pól elektromagnetycznych w środowisku, Dz.U. 2019 poz. 2448 oraz przepisy wykonawcze dotyczące sposobów sprawdzania dotrzymania dopuszczalnych poziomów pól elektromagnetycznych. Wymaganie obejmuje analizę i pomiary PEM dla stacji radiokomunikacyjnych, anten VHF/AIS, radiolinii, urządzeń nadawczo-odbiorczych i innych źródeł emisji.
10) W projekcie stosuje się zasadę „nie czyń poważnych szkód” DNSH, wymagania gospodarki obiegu zamkniętego, ograniczania ilości odpadów, energooszczędności,

trwałości, naprawialności i możliwości późniejszej wymiany komponentów w zakresie wynikającym z przepisów oraz dokumentów programowych finansowania projektu.

1.2.1.7. Wymagania dotyczące łączności elektronicznej, radiokomunikacji i zgodności urządzeń

1) Dla sieci, usług, urządzeń i infrastruktury łączności elektronicznej stosuje się ustawę z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej, Dz.U. 2024 poz. 1221 z późniejszymi zmianami oraz ustawę z dnia 12 lipca 2024 r. – Przepisy wprowadzające ustawę – Prawo komunikacji elektronicznej, Dz.U. 2024 poz. 1222. Wymaganie obejmuje zasady korzystania z częstotliwości, urządzeń radiowych, pozwoleń radiowych, tajemnicy komunikacji elektronicznej, bezpieczeństwa i współpracy z Prezesem UKE w zakresie właściwym dla systemu.
2) Dla urządzeń radiowych używanych bez pozwolenia radiowego stosuje się Rozporządzenie Ministra Cyfryzacji z dnia 9 lutego 2022 r. w sprawie urządzeń radiowych nadawczych lub nadawczo-odbiorczych, które mogą być używane bez pozwolenia radiowego, Dz.U. 2022 poz. 567 z późniejszymi zmianami, w tym zmianami ogłoszonymi w Dz.U. 2023 poz. 2567. Wymaganie obejmuje weryfikację dopuszczalnych zakresów częstotliwości, mocy, klas emisji, parametrów anten i warunków pracy urządzeń radiowych.
3) Dla urządzeń radiowych stosuje się Dyrektywę Parlamentu Europejskiego i Rady 2014/53/UE w sprawie harmonizacji ustawodawstw państw członkowskich dotyczących udostępniania na rynku urządzeń radiowych oraz krajowe przepisy wdrażające. Urządzenia radiowe dostarczane w ramach projektu muszą posiadać właściwe deklaracje zgodności UE, oznakowanie CE, instrukcje, parametry zgodne z przeznaczeniem i dokumentację potwierdzającą spełnienie zasadniczych wymagań.
4) Dla kompatybilności elektromagnetycznej stosuje się Dyrektywę 2014/30/UE, ustawę z dnia 13 kwietnia 2007 r. o kompatybilności elektromagnetycznej, Dz.U. 2025 poz. 180 oraz normy zharmonizowane właściwe dla urządzeń teleinformatycznych, radiowych, zasilających, CCTV, serwerowych i automatyki.
5) Dla bezpieczeństwa elektrycznego urządzeń w zakresie niskonapięciowym stosuje się Dyrektywę 2014/35/UE oraz właściwe przepisy krajowe i normy zharmonizowane. Wymaganie obejmuje urządzenia zasilające, UPS, rozdzielnice, zasilacze, osprzęt, szafy, urządzenia serwerowe i urządzenia terenowe.
6) Dla ograniczenia stosowania niektórych substancji niebezpiecznych w sprzęcie elektrycznym i elektronicznym stosuje się Dyrektywę 2011/65/UE RoHS, w brzmieniu zmienionym, oraz krajowe przepisy wdrażające. Sprzęt dostarczany w ramach projektu musi spełniać wymagania RoHS w zakresie mającym zastosowanie.
7) Dla systemu oceny zgodności i nadzoru rynku stosuje się ustawę z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, Dz.U. 2025 poz. 568, oraz Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1020 w sprawie nadzoru rynku i zgodności produktów. Wymaganie obejmuje dostarczenie urządzeń legalnie wprowadzonych do obrotu i udostępnionych na rynku UE.

8) Dla projektowania i eksploatacji radiolinii, transmisji radiowej, anten, torów antenowych i urządzeń radiowych stosuje się aktualne wymagania ITU, CEPT, ETSI, UKE, plany zagospodarowania częstotliwości oraz decyzje i pozwolenia radiowe właściwe dla danego zakresu częstotliwości i lokalizacji.

1.2.1.8. Wymagania dotyczące cyberbezpieczeństwa, danych, usług cyfrowych i dostępności

Generalny Wykonawca zobowiązany jest uwzględnić przepisy dotyczące krajowego systemu cyberbezpieczeństwa w brzmieniu obowiązującym na dzień wykonywania danej czynności, w tym przepisy wdrażające dyrektywę NIS2, o ile będą miały zastosowanie do Zamawiającego, systemu RIS, dostarczanych produktów ICT, usług ICT, procesów ICT albo usług utrzymania, bezpieczeństwa i monitorowania objętych przedmiotem zamówienia.

1) Dla cyberbezpieczeństwa systemu RIS stosuje się ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2026 poz. 20, wraz z ustawą z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, Dz.U. 2026 poz. 252. Wymaganie obejmuje środki organizacyjne i techniczne adekwatne do znaczenia systemu RIS, zarządzanie ryzykiem, zabezpieczenia sieci, usług, systemów informatycznych, urządzeń brzegowych, serwerów, systemów CCTV, VHF/AIS i transmisji, obsługę incydentów, monitorowanie, aktualizacje i dokumentowanie zabezpieczeń.
2) Dla minimalnych wymagań dla systemów teleinformatycznych, rejestrów publicznych, wymiany informacji w postaci elektronicznej oraz Krajowych Ram Interoperacyjności stosuje się Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. 2024 poz. 773, w okresie jego obowiązywania.
3) Dla ochrony danych osobowych stosuje się Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 RODO oraz ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz.U. 2019 poz. 1781 z późniejszymi zmianami. Wymaganie obejmuje ochronę danych w systemie CCTV, systemach operatorskich, kontach użytkowników, logach, systemach transmisyjnych, usługach cyfrowych, repozytoriach, kopiach zapasowych, dokumentacji i procesach utrzymaniowych.
4) Dla prywatności i poufności komunikacji elektronicznej stosuje się Dyrektywę 2002/58/WE oraz przepisy krajowe wynikające z Prawa komunikacji elektronicznej. Wymaganie obejmuje ochronę transmisji, ograniczenie nieuprawnionego dostępu, integralność komunikatów, kontrolę dostępu, audyt i rejestrowanie zdarzeń.
5) Dla dostępności cyfrowej stron internetowych, aplikacji mobilnych, portali, aplikacji mapowych, interfejsów użytkownika i usług cyfrowych udostępnianych użytkownikom stosuje się ustawę z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych, Dz.U. 2023 poz. 1440, oraz standard WCAG w zakresie wymaganym przepisami. Wymaganie obejmuje projektowanie, testowanie i dokumentowanie dostępności usług cyfrowych RIS.

6) Dla dostępności produktów i usług, jeżeli dostarczane rozwiązania mieszczą się w zakresie ustawowym, stosuje się ustawę z dnia 26 kwietnia 2024 r. o zapewnianiu spełniania wymagań dostępności niektórych produktów i usług przez podmioty gospodarcze, Dz.U. 2024 poz. 731. Wymaganie obejmuje produkty i usługi objęte zakresem ustawy od daty jej stosowania.
7) Dla otwartych danych, ponownego wykorzystywania informacji sektora publicznego, interfejsów udostępniania danych, metadanych i formatów maszynowo czytelnych stosuje się ustawę z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego, Dz.U. 2023 poz. 1524 z późniejszymi zmianami, w zakresie mającym zastosowanie do danych systemu RIS.
8) Dla projektowania API, wymiany danych, modelu uprawnień, usług integracyjnych, dokumentacji technicznej i mechanizmów udostępniania danych stosuje się zasady interoperacyjności, przenoszalności, otwartości, bezpieczeństwa, dokumentowalności i wersjonowania wynikające z KRI, Interoperable Europe Act, ES-RIS, RODO, Prawa komunikacji elektronicznej oraz standardów branżowych właściwych dla danego interfejsu.
9) Dla usług zaufania, podpisów elektronicznych, pieczęci elektronicznych, walidacji dokumentów elektronicznych i znakowania czasem, jeżeli są stosowane w systemie lub dokumentacji odbiorowej, stosuje się eIDAS oraz przepisy krajowe dotyczące usług zaufania i identyfikacji elektronicznej.
10) W zakresie bezpieczeństwa oprogramowania i urządzeń Generalny Wykonawca zapewni stosowanie aktualizacji bezpieczeństwa, konfiguracji utwardzającej, rozdziału uprawnień, mechanizmów uwierzytelniania, rejestrowania zdarzeń, szyfrowania transmisji, ochrony kopii zapasowych, zarządzania podatnościami i dokumentowania komponentów programowych w zakresie wymaganym przepisami, normami oraz architekturą systemu RIS.

1.2.1.9. Wymagania wynikające z finansowania, polityk horyzontalnych i oznakowania projektu

1) Dla projektu współfinansowanego ze środków Unii Europejskiej stosuje się Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1060 ustanawiające wspólne przepisy dla funduszy polityki spójności oraz przepisy właściwe dla Programu Fundusze Europejskie na Infrastrukturę, Klimat, Środowisko 2021–2027, w zakresie wynikającym z umowy o dofinansowanie, dokumentów programowych i obowiązków beneficjenta przeniesionych na realizację przedmiotu zamówienia.
2) Generalny Wykonawca zrealizuje oznakowanie produktów projektu, dokumentacji, infrastruktury, materiałów informacyjnych, interfejsów, tablic, naklejek i innych elementów wymagających oznaczenia zgodnie z obowiązującymi zasadami informacji i promocji dla Programu Fundusze Europejskie na Infrastrukturę, Klimat, Środowisko 2021–2027 oraz z zasadami oznaczania przedsięwzięć dofinansowanych przez Unię Europejską.
3) W zakresie zasady równości szans i niedyskryminacji, dostępności dla osób z niepełnosprawnościami, zgodności z Kartą Praw Podstawowych, zrównoważonego rozwoju, DNSH, efektywności energetycznej, gospodarki obiegu zamkniętego oraz

odporności klimatycznej stosuje się wymagania prawa unijnego, prawa krajowego, dokumentów programowych FEnIKS 2021–2027 i umowy o dofinansowanie w zakresie, w jakim dotyczą realizacji przedmiotu zamówienia.

1.2.1.10. Wymagania normatywne i standardy techniczne dla usług RIS

1) Dla architektury usług RIS, danych referencyjnych, RIS Index, wymiany danych, zgodności z EuRIS oraz interoperacyjności krajowej i europejskiej stosuje się aktualny ES-RIS oraz dokumenty techniczne CESNI powiązane z ES-RIS. System po rozbudowie musi umożliwiać zachowanie jednorodności z istniejącym systemem RIS Odra oraz wymianę danych z międzynarodowymi środowiskami RIS zgodnie z właściwymi specyfikacjami.
2) Dla Inland ECDIS i Inland ENC stosuje się aktualne wymagania ES-RIS, specyfikacje Inland ENC, standardy IHO właściwe dla danych hydrograficznych i elektronicznych map nawigacyjnych, w tym S-57, S-100, S-101/S-401 w zakresie ich stosowania, oraz standardy dystrybucji, walidacji i prezentacji map wymagane przez środowisko RIS.
3) Dla danych przestrzennych stosuje się właściwe standardy INSPIRE, ISO 19100, GML, systemy odniesienia przestrzennego obowiązujące w Polsce oraz wymagania krajowej infrastruktury informacji przestrzennej. Dane przestrzenne tworzone albo przetwarzane w systemie RIS muszą posiadać spójne identyfikatory, metadane, układ odniesienia, dokładność i mechanizmy aktualizacji.
4) Dla komunikatów dla kierowników statków stosuje się aktualne wymagania ES-RIS i właściwe specyfikacje NtS. Komunikaty muszą być tworzone, kodowane, walidowane, publikowane, pobierane i archiwizowane w formatach oraz strukturach dopuszczonych przez aktualny standard RIS.
5) Dla elektronicznego raportowania statków stosuje się aktualne wymagania ES-RIS, Rozporządzenie wykonawcze Komisji (UE) 2019/1744 oraz powiązane podręczniki implementacyjne wiadomości ERI. System musi zapewniać zgodność słowników, kodów, struktur komunikatów i walidacji z obowiązującymi specyfikacjami.
6) Dla śledzenia i namierzania statków stosuje się aktualne wymagania ES-RIS, Rozporządzenie wykonawcze Komisji (UE) 2019/838, standardy Inland AIS, aktualne rekomendacje ITU-R dotyczące AIS oraz właściwe normy IEC dla stacji AIS i interfejsów danych.

1.2.1.11. Wymagania normatywne dla VHF, AIS, DGNSS i infrastruktury antenowej

1) Dla stacji bazowych AIS, stacji brzegowych AIS, urządzeń AtoN AIS, interfejsów AIS i transmisji komunikatów AIS stosuje się aktualne normy IEC 62320, IEC 61993, IEC 61162, IEC 60945, aktualne rekomendacje ITU-R M.1371 oraz wymagania ES-RIS i Inland AIS. Zakres stosowania obejmuje sprzęt, konfigurację, interfejsy, czasy, komunikaty, synchronizację, odporność środowiskową, testy i dokumentację.

2) Dla łączności głosowej VHF stosuje się Regulamin Radiokomunikacyjny ITU, właściwe rekomendacje ITU-R, wymagania CEPT, RAINWAT w zakresie mającym zastosowanie do radiotelefonicznej służby na śródlądowych drogach wodnych, przepisy UKE, pozwolenia radiowe, plany zagospodarowania częstotliwości oraz normy ETSI właściwe dla radiotelefonów i stacji bazowych VHF.

3) Dla dystrybucji poprawek DGNSS stosuje się aktualne standardy RTCM SC-104, właściwe rekomendacje IALA dotyczące DGNSS oraz normy i specyfikacje wymagane przez dostarczane urządzenia i komponenty RIS. Wymaganie obejmuje format komunikatów, jakość danych, dostępność, opóźnienia, integralność i monitorowanie transmisji poprawek.

4) Dla projektowania torów antenowych stosuje się normy i standardy dotyczące kabli koncentrycznych, złączy, odgromników, uziemień, ochrony przepięciowej, separacji anten, odporności środowiskowej, strat toru i kompatybilności elektromagnetycznej. Dobór urządzeń i materiałów musi zapewniać zachowanie parametrów link budget, wymaganych zasięgów i dopuszczalnych poziomów emisji.

5) Dla wież, masztów, konstrukcji wsporczych, wsporników anten, pomostów, drabin, instalacji asekuracyjnych i elementów dostępowych stosuje się Eurokody, normy wykonania konstrukcji stalowych, normy zabezpieczenia antykorozyjnego, normy obciążenia wiatrem, oblodzeniem i temperaturą oraz wymagania BHP dla pracy na wysokości.

1.2.1.12. Wymagania normatywne dla systemu monitoringu wizyjnego CCTV/VSS

1) Dla systemu monitoringu wizyjnego stosuje się serię PN-EN IEC 62676 dotyczącą systemów dozorowych w zastosowaniach zabezpieczeniowych, w szczególności wymagania systemowe, transmisję wideo IP, protokoły, interoperacyjność, jakość obrazu, konfigurację, dokumentację, testy i wytyczne stosowania. Stosowanie historycznych norm PN-EN 50132 następuje wyłącznie w zakresie, w jakim nie zostały zastąpione przez serię PN-EN IEC 62676 i nie pozostają sprzeczne z aktualnymi standardami.

2) Dla kompatybilności urządzeń CCTV stosuje się ONVIF Profile S, T, G i M albo profile równoważne właściwe dla kamer, rejestratorów, VMS, analityki obrazu, metadanych i integracji API. Interfejsy muszą umożliwiać strumieniowanie, sterowanie PTZ, konfigurację, zdarzenia, alarmy, metadane, synchronizację czasu i monitorowanie stanu urządzeń.

3) Dla kodowania i transmisji strumieni wideo stosuje się właściwe standardy ISO/IEC i ITU-T dotyczące H.264/AVC, H.265/HEVC albo nowszych kodeków dopuszczonych w projekcie, a także protokoły RTSP, RTP, SRTP, HTTPS, TLS i inne bezpieczne protokoły transmisji w zakresie wynikającym z architektury CCTV.

4) Dla urządzeń CCTV stosuje się normy odporności środowiskowej, szczelności i wytrzymałości mechanicznej, w szczególności PN-EN IEC 60529 dla stopni ochrony IP, PN-EN IEC 62262 dla odporności IK, normy temperatury pracy, odporności na wilgotność, korozję, wibracje i promieniowanie UV oraz normy kompatybilności elektromagnetycznej właściwe dla urządzeń elektronicznych.

5) Dla systemu rejestracji, archiwizacji, eksportu, retencji, uwierzytelniania, kontroli dostępu i logowania zdarzeń w CCTV stosuje się RODO, KSC, KRI, normy cyberbezpieczeństwa, wymagania dowodowe i wymagania integralności nagrań. System musi umożliwiać kontrolę dostępu do obrazu na żywo, nagrań archiwalnych, eksportów, konfiguracji i metadanych.

1.2.1.13. Wymagania normatywne dla sieci transmisyjnej, VPN i infrastruktury IP

1) Dla warstwy Ethernet stosuje się standardy IEEE 802.3, IEEE 802.1Q, IEEE 802.1p, IEEE 802.1X i inne właściwe standardy IEEE wymagane dla przełączania, segmentacji, kontroli dostępu, QoS, agregacji łączy i zasilania PoE.
2) Dla adresacji, routingu, separacji, bezpieczeństwa transmisji i komunikacji IP stosuje się aktualne standardy IETF/RFC dotyczące IPv4, IPv6, TCP, UDP, ICMP, DNS, DHCP, NTP, SNMPv3, SSH, syslog, IPsec, TLS 1.2/1.3, HTTPS, VPN, QoS i mechanizmów redundancji. Protokoły przestarzałe, słabe kryptograficznie albo niewspierane bezpieczeństwa nie mogą być stosowane do komunikacji produkcyjnej.
3) Dla sieci VPN stosuje się IPsec, IKEv2, TLS VPN albo rozwiązania równoważne zapewniające szyfrowanie, uwierzytelnianie, integralność, separację ruchu, wymianę kluczy zgodną z aktualnymi zaleceniami kryptograficznymi oraz możliwość audytu konfiguracji.
4) Dla okablowania strukturalnego, światłowodowego i miedzianego stosuje się ISO/IEC 11801, PN-EN 50173, PN-EN 50174, PN-EN 50310 oraz normy dotyczące pomiarów torów transmisyjnych. Wymaganie obejmuje projekt, dobór kategorii i klas, trasy kablowe, promienie gięcia, separację od instalacji energetycznych, pomiary, oznaczenia i dokumentację powykonawczą.
5) Dla radiolinii, łączy LTE/5G, połączeń operatorowych, APN, routerów wielotorowych i połączeń zapasowych stosuje się właściwe normy ETSI, 3GPP, wymagania operatorów telekomunikacyjnych, wymagania UKE, zasady bezpieczeństwa transmisji i wymagania dotyczące monitorowania dostępności oraz jakości łącza.
6) Dla monitorowania sieci stosuje się standardy SNMPv3, syslog, NetFlow/IPFIX albo równoważne, NTP/PTP dla synchronizacji czasu oraz mechanizmy alarmowania, archiwizacji logów i raportowania dostępności wymagane przez KSC, KRI i dokumentację eksploatacyjną systemu RIS.

1.2.1.14. Wymagania normatywne dla serwerowni, infrastruktury serwerowej i ciągłości działania

1) Dla serwerowni, pomieszczeń technicznych, szaf, zasilania, chłodzenia, tras kablowych, bezpieczeństwa fizycznego i utrzymania ciągłości działania stosuje się serię PN-EN 50600 oraz ISO/IEC 22237 w zakresie właściwym dla skali i klasy projektowanego rozwiązania. Dopuszcza się stosowanie TIA-942 jako standardu uzupełniającego albo równoważnego, jeżeli nie obniża wymagań PFU.

2) Dla zasilania gwarantowanego i UPS stosuje się serię PN-EN IEC 62040, normy bezpieczeństwa elektrycznego, kompatybilności elektromagnetycznej, odporności środowiskowej oraz wymagania producentów urządzeń. Wymaganie obejmuje dobór mocy, autonomię, zabezpieczenia, bypass, baterie, monitoring, testy obciążeniowe i bezpieczną wymianę modułów bateryjnych.
3) Dla instalacji elektrycznych niskiego napięcia stosuje się serię PN-HD 60364, normy PN-EN IEC 61439 dla rozdzielnic, PN-EN IEC 61643 dla ograniczników przepięć, PN-EN 62305 dla ochrony odgromowej oraz normy dotyczące uziemień i połączeń wyrównawczych.
4) Dla sprzętu serwerowego, macierzy dyskowych, systemów backupu, przełączników, zapór sieciowych, urządzeń UTM, koncentratorów VPN i platform wirtualizacyjnych stosuje się normy producentów, normy bezpieczeństwa IT, normy EMC, wymagania cyberbezpieczeństwa, wymagania zgodności produktu oraz wymagania interoperacyjności z istniejącym środowiskiem systemu RIS.
5) Dla kopii zapasowych, odtwarzania po awarii, replikacji, archiwizacji i testów odtworzeniowych stosuje się normy ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27031 oraz dobre praktyki właściwe dla ciągłości działania systemów teleinformatycznych. Wymaganie obejmuje definicję RPO, RTO, retencji, separacji kopii, szyfrowania, kontroli dostępu i regularnego testowania odtworzeń.

1.2.1.15. Wymagania normatywne dla konstrukcji, posadowienia i ochrony antykorozyjnej

1) Dla projektowania konstrukcji stosuje się Eurokody, w szczególności PN-EN 1990, PN-EN 1991, PN-EN 1992, PN-EN 1993, PN-EN 1993-3-1, PN-EN 1997 i PN-EN 1998 w zakresie właściwym dla rodzaju konstrukcji, posadowienia, strefy obciążeń, warunków gruntowych i oddziaływań środowiskowych.
2) Dla wykonania konstrukcji stalowych stosuje się PN-EN 1090-1 i PN-EN 1090-2, wymagania dotyczące klasy wykonania EXC, spawania, kontroli jakości, tolerancji, dokumentacji materiałowej, deklaracji właściwości użytkowych oraz oznakowania CE elementów konstrukcyjnych.
3) Dla zabezpieczeń antykorozyjnych stosuje się PN-EN ISO 12944, PN-EN ISO 1461, PN-EN ISO 14713, PN-EN ISO 8501, PN-EN ISO 9223 i normy powiązane. Wymaganie obejmuje określenie kategorii korozyjności środowiska, trwałości zabezpieczenia, przygotowania powierzchni, cynkowania, powłok malarskich, kontroli grubości i dokumentacji jakości.
4) Dla obciążeń wiatrem, śniegiem, oblodzeniem, temperaturą i oddziaływaniami eksploatacyjnymi stosuje się aktualne Eurokody i załączniki krajowe. Historyczne normy PN-B dotyczące wież, masztów, wiatru, oblodzenia i temperatury nie stanowią podstawowego odniesienia projektowego, jeżeli zostały zastąpione Eurokodami.
5) Dla bezpieczeństwa dostępu, drabin, podestów, urządzeń asekuracyjnych, pracy na wysokości i ewakuacji stosuje się właściwe normy PN-EN dotyczące środków dostępu stałego, ochrony przed upadkiem z wysokości, urządzeń kotwiczących i wymagań BHP.

1.2.1.16. Wymagania normatywne dla zasilania, ochrony odgromowej, uziemień i ochrony przepięciowej

1) Instalacje elektryczne muszą być zaprojektowane, wykonane, zbadane i odebrane zgodnie z serią PN-HD 60364, właściwymi warunkami przyłączenia, przepisami Prawa energetycznego, wymaganiami operatorów systemów dystrybucyjnych oraz przepisami BHP i ochrony przeciwpożarowej.
2) Ochronę odgromową projektuje się i wykonuje zgodnie z serią PN-EN 62305. Wymaganie obejmuje analizę ryzyka, dobór poziomu ochrony LPS, zwody, przewody odprowadzające, uziemienie, połączenia wyrównawcze, ochronę urządzeń elektronicznych i koordynację ochrony przepięciowej.
3) Ograniczniki przepięć i ochrona urządzeń teleinformatycznych, radiowych, CCTV, zasilających i antenowych muszą spełniać właściwe części serii PN-EN IEC 61643 oraz normy dotyczące ochrony torów sygnałowych, telekomunikacyjnych, zasilających i antenowych.
4) Szafy zasilające, rozdzielnice, obudowy i wyposażenie elektryczne muszą spełniać PN-EN IEC 61439, PN-EN IEC 60529, PN-EN IEC 62262 oraz normy bezpieczeństwa elektrycznego i kompatybilności elektromagnetycznej właściwe dla miejsca instalacji.
5) Dla instalacji fotowoltaicznych, jeżeli zostaną zastosowane, stosuje się właściwe przepisy Prawa budowlanego, Prawa energetycznego, normy PN-HD 60364-7-712, PN-EN IEC 62446, PN-EN IEC 61215, PN-EN IEC 61730, normy ochrony przeciwpożarowej, ochrony odgromowej i ochrony przepięciowej oraz wymagania operatora sieci.

1.2.1.17. Wymagania normatywne dla cyberbezpieczeństwa, jakości oprogramowania i testów

1) Dla systemowego zarządzania bezpieczeństwem informacji stosuje się PN-EN ISO/IEC 27001, PN-EN ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 27017, ISO/IEC 27018 i ISO/IEC 27701 w zakresie właściwym dla architektury, modelu przetwarzania danych, środowiska chmurowego, usług utrzymania i ochrony prywatności.
2) Dla systemów automatyki, urządzeń terenowych, stacji brzegowych, komponentów przemysłowych, zasilania, monitoringu technicznego i infrastruktury krytycznej stosuje się serię IEC 62443 w zakresie właściwym dla architektury i klasy ryzyka. Wymaganie obejmuje segmentację, strefy i kanały komunikacyjne, poziomy bezpieczeństwa, zarządzanie podatnościami i bezpieczny cykl życia komponentów.
3) Dla urządzeń połączonych z siecią, kamer IP, bramek, routerów, modemów, urządzeń IoT i systemów wbudowanych stosuje się ETSI EN 303 645 oraz inne właściwe standardy cyberbezpieczeństwa urządzeń połączonych. Wymaganie obejmuje unikalne dane uwierzytelniające, aktualizacje, bezpieczną konfigurację, ochronę danych i ograniczenie nieużywanych usług.
4) Dla bezpieczeństwa aplikacji webowych, API, portali, aplikacji mapowych i interfejsów administracyjnych stosuje się OWASP ASVS, OWASP Top 10, OWASP API Security Top

10, dobre praktyki bezpiecznego programowania, testy SAST/DAST, testy podatności oraz wymagania kryptograficzne zgodne z aktualnym stanem wiedzy.

5) Dla jakości oprogramowania stosuje się ISO/IEC 25010, ISO/IEC/IEEE 12207, ISO/IEC/IEEE 15288 i ISO/IEC/IEEE 29148 w zakresie wymagań, projektowania, wytwarzania, testowania, utrzymania, dokumentowania i zarządzania konfiguracją. Wymaganie obejmuje czytelne wymagania funkcjonalne i niefunkcjonalne, testowalność, śledzenie wymagań i kontrolę wersji.
6) Testy systemu RIS muszą obejmować testy jednostkowe, integracyjne, systemowe, akceptacyjne, wydajnościowe, bezpieczeństwa, odporności, ciągłości działania, odtworzeniowe, kompatybilności, interoperacyjności i zgodności normatywnej. Wyniki testów muszą być udokumentowane protokołami i raportami umożliwiającymi potwierdzenie spełnienia wymagań PFU.

1.2.1.18. Wymagania dotyczące dokumentów zgodności, odbiorów i przekazania do eksploatacji

1) Generalny Wykonawca przygotuje i przekaże dokumentację projektową, wykonawczą, powykonawczą, eksploatacyjną, administracyjną i odbiorową w zakresie umożliwiającym potwierdzenie zgodności prawnej, normatywnej, technicznej, funkcjonalnej i cyberbezpieczeństwa całego przedmiotu zamówienia.
2) Dla każdego urządzenia, wyrobu, systemu i komponentu Generalny Wykonawca przekaże deklaracje zgodności UE, deklaracje właściwości użytkowych, certyfikaty, atesty, karty katalogowe, instrukcje, dokumenty dopuszczające, licencje, warunki gwarancji, dokumentację bezpieczeństwa, dokumentację aktualizacji i dokumentację konfiguracji, w zakresie wymaganym dla danej kategorii produktu.
3) Dla robót budowlanych i instalacyjnych Generalny Wykonawca przekaże dokumentację powykonawczą, geodezyjną inwentaryzację powykonawczą, protokoły badań i pomiarów, protokoły odbiorów branżowych, dokumentację materiałową, potwierdzenia wykonania zabezpieczeń antykorozyjnych, protokoły uziemień, ochrony odgromowej, ochrony przepięciowej, instalacji elektrycznych, instalacji telekomunikacyjnych i pomiarów torów transmisyjnych.
4) Dla systemów teleinformatycznych Generalny Wykonawca przekaże dokumentację architektury, konfiguracji, adresacji, segmentacji, zasad dostępu, kont uprzywilejowanych, integracji, API, usług, certyfikatów, kopii zapasowych, polityk aktualizacji, procedur odtworzeniowych, logowania, monitoringu, raportowania i obsługi incydentów.
5) Dla systemów VHF/AIS Generalny Wykonawca przekaże dokumentację radiową, projekt antenowy, wyniki analiz propagacyjnych, dokumenty pozwoleniowe, parametry torów antenowych, protokoły strojenia, protokoły pomiarów, konfiguracje stacji, wykaz kanałów, wykaz MMSI/identyfikatorów, protokoły testów zasięgu, komunikatów AIS, łączności VHF i dystrybucji poprawek DGNSS.
6) Dla systemu CCTV Generalny Wykonawca przekaże dokumentację lokalizacji kamer, pól widzenia, strumieni, profili kodowania, retencji, kont użytkowników, uprawnień, integracji ONVIF/API, rejestracji, archiwizacji, eksportu, monitoringu dostępności, testów jakości obrazu, testów PTZ, testów dostępności nagrań i testów bezpieczeństwa.

7) Dla systemu transmisyjnego Generalny Wykonawca przekaże dokumentację topologii fizycznej i logicznej, wykaz łączy, wykaz urządzeń, konfiguracje, parametry SLA, parametry QoS, trasy podstawowe i zapasowe, zasady przełączenia awaryjnego, adresację, VLAN, reguły zapór, tunele VPN, wyniki testów przepustowości, opóźnień, utraty pakietów, dostępności i bezpieczeństwa.
8) Przekazanie do eksploatacji wymaga potwierdzenia zgodności z przepisami, normami, decyzjami administracyjnymi, pozwoleniami, warunkami przyłączenia, wymaganiami cyberbezpieczeństwa, wymaganiami dostępności, wymaganiami ochrony danych i wymaganiami interoperacyjności RIS. Potwierdzenie następuje poprzez komplet dokumentów, protokołów, testów, oświadczeń i wyników pomiarów.

1.2.1.19. Wymagania dotyczące aktualizacji wykazu przepisów i norm w toku realizacji

1) Generalny Wykonawca jest zobowiązany do utrzymywania aktualności stosowanych podstaw prawnych i normatywnych przez cały okres realizacji zamówienia. Dotyczy to w szczególności zmian przepisów RIS, Prawa komunikacji elektronicznej, cyberbezpieczeństwa, Prawa budowlanego, ochrony środowiska, ochrony danych osobowych, przepisów radiowych, norm zharmonizowanych, Eurokodów oraz standardów branżowych dla AIS, VHF, CCTV, transmisji danych i serwerowni.
2) W przypadku wejścia w życie nowych przepisów albo norm, które mają zastosowanie do projektowanych, dostarczanych albo wykonywanych elementów, Generalny Wykonawca uwzględni je w dokumentacji, doborze urządzeń, konfiguracji, testach i odbiorach, o ile przepisy przejściowe nie stanowią inaczej.
3) W dokumentacji odbiorowej Generalny Wykonawca potwierdzi, że zastosowane akty prawne, normy i standardy były aktualne na moment wykonania danego elementu oraz że ewentualne odstępstwa, równoważności albo zastosowanie norm zastępujących zostały jednoznacznie wykazane i uzasadnione technicznie.

1.2.2. Zasady projektowania

1) Generalny Wykonawca zobowiązany jest zaprojektować przedmiot zamówienia jako jeden spójny, zintegrowany i skalowalny system RIS, obejmujący infrastrukturę terenową, systemy radiokomunikacyjne VHF/AIS/DGNSS, system monitoringu wizyjnego CCTV, czujniki hydrologiczne i meteorologiczne, sieć transmisji danych, infrastrukturę serwerową, środowiska systemowe, usługi cyfrowe, mechanizmy integracyjne, systemy bezpieczeństwa, monitoring techniczny oraz dokumentację niezbędną do budowy, wdrożenia, odbioru i późniejszej eksploatacji systemu.
2) Projektowanie musi być prowadzone zgodnie z formułą „zaprojektuj i zbuduj”. Oznacza to, że Generalny Wykonawca ponosi odpowiedzialność za dobór rozwiązań technicznych, technologicznych, materiałowych, konstrukcyjnych, systemowych, aplikacyjnych i organizacyjnych, o ile spełniają one wymagania PFU, wymagania dokumentów branżowych, obowiązujące przepisy prawa, normy, standardy techniczne, warunki zarządców obiektów i nieruchomości oraz wymagania Zamawiającego.

3) Generalny Wykonawca nie może traktować PFU, planów branżowych, wykazów lokalizacji, analiz propagacyjnych, analiz transmisyjnych, inwentaryzacji i materiałów referencyjnych jako dokumentacji zwalniającej z obowiązku wykonania własnych analiz, obliczeń, wizji lokalnych, uzgodnień, pomiarów, projektów, ekspertyz oraz weryfikacji technicznej. Dokumenty te stanowią materiał wejściowy do projektowania oraz określają minimalny, oczekiwany przez Zamawiającego poziom funkcjonalny, techniczny i jakościowy rozwiązania.
4) Na etapie projektowania Generalny Wykonawca zobowiązany jest zweryfikować aktualność wszystkich danych wejściowych, w szczególności:
    a) lokalizacji wskazanych w PFU i załącznikach;
    b) stanu technicznego obiektów, konstrukcji i infrastruktury istniejącej;
    c) warunków terenowych, konstrukcyjnych, geotechnicznych, hydrologicznych, środowiskowych i dostępności serwisowej;
    d) możliwości doprowadzenia zasilania i transmisji danych;
    e) możliwości montażu urządzeń, anten, kamer, czujników, szaf teletechnicznych i tras kablowych;
    f) występowania kolizji z istniejącą infrastrukturą;
    g) warunków ochrony odgromowej, uziemienia, ochrony przepięciowej i kompatybilności elektromagnetycznej;
    h) wymagań zarządców nieruchomości, obiektów mostowych, hydrotechnicznych, drogowych, kolejowych oraz gestorów sieci;
    i) wymagań formalnych dotyczących decyzji, zgłoszeń, pozwoleń, opinii, uzgodnień i warunków technicznych;
    j) aktualności założeń propagacyjnych, transmisyjnych, przepustowościowych i funkcjonalnych.
5) W przypadku stwierdzenia przez Generalnego Wykonawcę rozbieżności pomiędzy PFU, dokumentami branżowymi, stanem faktycznym, stanem prawnym, wymaganiami zarządców albo możliwościami technicznymi danej lokalizacji, Generalny Wykonawca zobowiązany jest niezwłocznie przedstawić Zamawiającemu opis rozbieżności, ocenę wpływu na realizację przedmiotu zamówienia oraz propozycję rozwiązania zamiennego lub korygującego. Rozwiązanie zamienne może zostać zastosowane wyłącznie po uzyskaniu akceptacji Zamawiającego i nie może prowadzić do obniżenia funkcjonalności, niezawodności, bezpieczeństwa, interoperacyjności, trwałości ani jakości systemu RIS.
6) Projektowanie musi uwzględniać zasadę minimalizacji ingerencji w istniejącą infrastrukturę systemu RIS, przy jednoczesnym zapewnieniu pełnej integracji nowych, modernizowanych i wykorzystywanych ponownie elementów systemu. Generalny Wykonawca zobowiązany jest jednoznacznie określić w dokumentacji projektowej:
    a) elementy nowe;
    b) elementy modernizowane;
    c) elementy wymieniane;
    d) elementy istniejące wykorzystywane bez ingerencji;

e) elementy istniejące wykorzystywane po rekonfiguracji;

f) elementy istniejące objęte odpowiedzialnością Generalnego Wykonawcy;

g) elementy istniejące pozostające poza zakresem odpowiedzialności Generalnego Wykonawcy.

7) Projektowanie musi zapewniać zachowanie ciągłości działania obecnego systemu RIS w zakresie niezbędnym dla bieżącej działalności Zamawiającego. Generalny Wykonawca zobowiązany jest tak planować prace projektowe, montażowe, instalacyjne, konfiguracyjne, migracyjne i testowe, aby ograniczyć ryzyko przerw w działaniu systemów istniejących. Czynności mogące wpływać na dostępność usług RIS wymagają wcześniejszego uzgodnienia z Zamawiającym, określenia okna serwisowego, procedury wycofania zmiany oraz sposobu potwierdzenia przywrócenia prawidłowej pracy systemu.

8) Rozwiązania projektowe muszą być projektowane z uwzględnieniem zasady odporności operacyjnej systemu RIS. Wymaga się, aby projekt uwzględniał redundancję, mechanizmy przełączenia awaryjnego, zasilanie rezerwowe, nadzór techniczny, alarmowanie, możliwość diagnostyki zdalnej, możliwość odtworzenia konfiguracji, możliwość odtworzenia danych oraz możliwość bezpiecznej aktualizacji oprogramowania i konfiguracji w okresie eksploatacji.

9) Dla podsystemu VHF/AIS/DGNSS Generalny Wykonawca zobowiązany jest zaprojektować rozwiązanie w sposób zapewniający pokrycie funkcjonalne wymaganych odcinków Odrzańskiej Drogi Wodnej, prawidłową pracę stacji brzegowych, właściwą separację anten, właściwe parametry torów antenowych, prawidłową propagację sygnału, zgodność z pozwoleniami radiowymi, kompatybilność z istniejącymi komponentami systemu RIS oraz możliwość centralnego nadzoru, sterowania, rejestracji, alarmowania i diagnostyki. Projekt musi obejmować co najmniej analizę propagacyjną, projekt antenowy, projekt torów antenowych, projekt zasilania, projekt transmisji danych, projekt integracji z systemami centralnymi oraz projekt testów zasięgu i funkcji radiowych.

10) Dla podsystemu CCTV Generalny Wykonawca zobowiązany jest zaprojektować rozmieszczenie kamer, pola widzenia, kierunki obserwacji, parametry optyczne, parametry strumieni wideo, retencję, rejestrację, archiwizację, zasady eksportu materiału, maski prywatności, uprawnienia użytkowników, integrację z systemem RIS, monitoring techniczny oraz testy scenariuszowe. Projekt punktu kamerowego musi uwzględniać cel obserwacji, wymagany obszar widoczności, ograniczenia montażowe, stabilność konstrukcji, odporność środowiskową, dostęp serwisowy, transmisję danych, zasilanie, ochronę przed dostępem osób nieuprawnionych oraz ochronę prywatności.

11) Dla sieci transmisji danych Generalny Wykonawca zobowiązany jest zaprojektować architekturę komunikacji pomiędzy lokalizacjami terenowymi, obiektami pośrednimi, serwerownią główną, serwerownią zapasową, Centrum RIS oraz pozostałymi środowiskami systemowymi. Projekt musi uwzględniać wymagania przepustowościowe wynikające z liczby i rodzaju urządzeń, kamer, sensorów, stacji radiowych, usług cyfrowych i mechanizmów monitoringu technicznego. Projekt musi również uwzględniać bezpieczeństwo transmisji, separację ruchu, segmentację sieci, reguły dostępu, szyfrowanie, tunele VPN, adresację, nazewnictwo, QoS, monitoring, diagnostykę, redundancję torów dostępowych, przełączanie awaryjne oraz skalowalność.

12) Generalny Wykonawca zobowiązany jest projektować wszystkie nowe i modernizowane lokalizacje terenowe jako kompletne punkty infrastruktury RIS. Oznacza to, że projekt nie może ograniczać się wyłącznie do wskazania urządzeń końcowych, lecz musi obejmować również:
    a) konstrukcje wsporcze;
    b) fundamenty lub sposób mocowania;
    c) szafy teletechniczne;
    d) zasilanie podstawowe i rezerwowe;
    e) instalacje elektryczne;
    f) uziemienie, ochronę odgromową i ochronę przepięciową;
    g) trasy kablowe;
    h) tory antenowe;
    i) transmisję danych;
    j) zabezpieczenia fizyczne;
    k) monitoring techniczny;
    l) dostęp serwisowy;
    m) oznakowanie infrastruktury;
    n) wymagania BHP;
    o) wymagania środowiskowe;
    p) wymagania formalne wynikające z lokalizacji na danym obiekcie lub nieruchomości.
13) W przypadku projektowania infrastruktury na obiektach mostowych, hydrotechnicznych, drogowych, kolejowych, budynkach, wieżach, masztach albo innych konstrukcjach istniejących Generalny Wykonawca zobowiązany jest wykonać ocenę możliwości wykorzystania danej konstrukcji. Ocena musi obejmować w szczególności nośność, stateczność, wpływ obciążeń dodatkowych, wpływ wiatru, wpływ drgań, sposób mocowania, możliwość prowadzenia tras kablowych, dostęp serwisowy, bezpieczeństwo użytkowników obiektu, wpływ na funkcje podstawowe obiektu oraz wymagania jego zarządcy.
14) W przypadku projektowania wież, masztów, słupów kamerowych i konstrukcji wsporczych Generalny Wykonawca zobowiązany jest wykonać projekt dostosowany do warunków lokalnych, w tym warunków gruntowo-wodnych, strefy wiatrowej, oblodzenia, kategorii geotechnicznej, sposobu posadowienia, strefy przemarzania, warunków hydrologicznych, dostępu serwisowego, wymagań zarządcy terenu oraz wymagań eksploatacyjnych systemu RIS. Zastosowanie rozwiązania typowego wymaga jego pełnej adaptacji do konkretnej lokalizacji.
15) W przypadku projektowania infrastruktury na nieruchomościach lub obiektach zarządzanych przez PGW Wody Polskie, zarządców dróg, zarządców infrastruktury kolejowej, zarządców obiektów mostowych, zarządców obiektów hydrotechnicznych albo innych właścicieli i użytkowników infrastruktury, Generalny Wykonawca zobowiązany jest

uwzględnić wszystkie warunki techniczne, organizacyjne, eksploatacyjne i formalne wskazane przez danego zarządcę. Dokumentacja projektowa musi być przygotowana w zakresie umożliwiającym uzyskanie wymaganych zgód, uzgodnień, decyzji, pozwoleń i warunków realizacji.

16) Projektowanie musi uwzględniać ochronę ludzi, mienia, środowiska i infrastruktury istniejącej. Generalny Wykonawca zobowiązany jest uwzględnić w projektach wymagania dotyczące bezpieczeństwa konstrukcji, bezpieczeństwa pożarowego, ochrony przeciwporażeniowej, ochrony odgromowej, ochrony przepięciowej, kompatybilności elektromagnetycznej, pól elektromagnetycznych, ochrony środowiska, gospodarki odpadami, ochrony wód, ochrony danych osobowych, cyberbezpieczeństwa oraz bezpieczeństwa pracy ekip montażowych i serwisowych.

17) Projektowanie usług cyfrowych, interfejsów, API, modeli danych, mechanizmów integracyjnych i wymiany danych musi być prowadzone w sposób zapewniający interoperacyjność techniczną, semantyczną, organizacyjną i prawną. Rozwiązania muszą wspierać integrację z systemem RIS, systemami centralnymi Zamawiającego, środowiskami operatorskimi, podsystemami terenowymi, usługami VTT, informacją hydrometeorologiczną, danymi AIS, CCTV oraz wymaganymi usługami krajowymi i europejskimi, w szczególności w zakresie właściwym dla RIS, ES-RIS i EuRIS.

18) Projektowanie systemu musi uwzględniać zasadę bezpieczeństwa od projektu. Generalny Wykonawca zobowiązany jest uwzględnić w dokumentacji projektowej co najmniej:

    a) segmentację sieci;
    b) model stref i kanałów komunikacyjnych;
    c) kontrolę dostępu;
    d) zarządzanie kontami i uprawnieniami;
    e) uwierzytelnianie i autoryzację;
    f) szyfrowanie transmisji;
    g) rejestrowanie zdarzeń;
    h) monitoring bezpieczeństwa;
    i) utwardzenie konfiguracji;
    j) zarządzanie podatnościami;
    k) aktualizacje bezpieczeństwa;
    l) kopie zapasowe;
    m) procedury odtworzeniowe;
    n) zasady postępowania z kontami uprzywilejowanymi;
    o) ograniczenie nieużywanych usług i interfejsów;
    p) wymagania bezpieczeństwa dla urządzeń terenowych, kamer IP, routerów, modemów, bramek, serwerów, aplikacji, API i systemów wbudowanych.

19) Generalny Wykonawca zobowiązany jest projektować system w sposób umożliwiający jego testowanie i odbiór. Każde wymaganie funkcjonalne, techniczne, bezpieczeństwa,

wydajnościowe, dostępnościowe, interoperacyjnościowe i eksploatacyjne musi mieć przypisany sposób weryfikacji. Dokumentacja projektowa musi umożliwiać przygotowanie scenariuszy testowych, protokołów odbioru, kryteriów akceptacji oraz raportów potwierdzających spełnienie wymagań.

20) Projektowanie musi uwzględniać wymagania eksploatacyjne systemu RIS. Rozwiązania muszą być zaprojektowane tak, aby umożliwiały Zamawiającemu bieżący nadzór, diagnostykę, obsługę zdarzeń, wykonywanie kopii zapasowych, odtwarzanie konfiguracji, zarządzanie aktualizacjami, wykonywanie przeglądów technicznych, prowadzenie konserwacji, dokumentowanie zmian oraz korzystanie z dokumentacji administratora, użytkownika i dokumentacji eksploatacyjnej.

21) Generalny Wykonawca zobowiązany jest projektować rozwiązania w sposób zapewniający trwałość, dostępność części zamiennych, wsparcie producenta, możliwość rozbudowy, możliwość wymiany komponentów, możliwość aktualizacji oprogramowania oraz możliwość utrzymania systemu w całym okresie gwarancji i eksploatacji. Niedopuszczalne jest projektowanie rozwiązań opartych na komponentach wycofanych, schyłkowych, niewspieranych, nieposiadających dokumentacji technicznej, nieposiadających aktualizacji bezpieczeństwa albo utrudniających utrzymanie systemu przez Zamawiającego.

22) Generalny Wykonawca zobowiązany jest zapewnić spójność dokumentacji projektowej pomiędzy branżami. Dokumentacja dotycząca obiektów, konstrukcji, zasilania, uziemień, ochrony odgromowej, torów antenowych, transmisji danych, CCTV, VHF/AIS/DGNSS, czujników, serwerowni, usług cyfrowych, cyberbezpieczeństwa i integracji musi być wzajemnie zgodna. W szczególności projekt nie może zawierać sprzecznych założeń dotyczących lokalizacji urządzeń, zapotrzebowania na moc, przepustowości, adresacji, tras kablowych, sposobu montażu, zakresu odpowiedzialności, testów albo odbiorów.

23) Dokumentacja projektowa musi być opracowana w zakresie i szczegółowości umożliwiającej uzyskanie wymaganych decyzji, pozwoleń, zgłoszeń, opinii, uzgodnień i warunków technicznych, wykonanie robót, przeprowadzenie odbiorów, przekazanie systemu do eksploatacji oraz późniejsze utrzymanie rozwiązania. Generalny Wykonawca zobowiązany jest przygotować w szczególności dokumentację projektową, wykonawczą, uzgodnieniową, konfiguracyjną, testową, powykonawczą, odbiorową i eksploatacyjną w zakresie właściwym dla przyjętego rozwiązania.

24) Wymagania dotyczące języka dokumentacji i prowadzenia projektu

    a) Generalny Wykonawca zobowiązany jest prowadzić całość procesu projektowania, realizacji, uzgodnień, dokumentowania, testowania, odbiorów i przekazania przedmiotu zamówienia do eksploatacji w języku polskim.

    b) Całość dokumentacji opracowywanej, przekazywanej, aktualizowanej lub uzupełnianej przez Generalnego Wykonawcę w ramach realizacji przedmiotu zamówienia musi zostać sporządzona w języku polskim. Wymóg ten dotyczy w szczególności dokumentacji projektowej, wykonawczej, powykonawczej, konfiguracyjnej, odbiorowej, testowej, eksploatacyjnej, administratora, użytkownika, serwisowej, szkoleniowej, gwarancyjnej, raportowej, uzgodnieniowej oraz korespondencji formalnej przekazywanej Zamawiającemu.

c) W przypadku dokumentów, instrukcji, certyfikatów, deklaracji zgodności, kart katalogowych, dokumentacji producenta, dokumentacji licencyjnej, dokumentacji API, dokumentacji technicznej urządzeń, oprogramowania lub usług, które zostały pierwotnie opracowane w języku obcym, Generalny Wykonawca zobowiązany jest zapewnić ich tłumaczenie na język polski w zakresie niezbędnym do prawidłowego projektowania, odbioru, eksploatacji, administracji, utrzymania, serwisowania, aktualizacji oraz oceny zgodności przedmiotu zamówienia. Zamawiający może dopuścić pozostawienie wybranych dokumentów technicznych w języku angielskim wyłącznie w przypadku, gdy mają one charakter pomocniczy, specjalistyczny albo producent nie udostępnia ich w języku polskim, a ich pozostawienie w języku angielskim nie ogranicza możliwości korzystania z systemu, jego eksploatacji, utrzymania, odbioru ani weryfikacji zgodności z PFU.

d) Językiem obowiązującym w toku realizacji projektu jest język polski. W języku polskim muszą być prowadzone w szczególności narady, warsztaty, spotkania robocze, konsultacje techniczne, prezentacje rozwiązań, przeglądy dokumentacji, uzgodnienia z Zamawiającym, szkolenia, testy, odbiory oraz komunikacja dotycząca realizacji przedmiotu zamówienia. Jeżeli Generalny Wykonawca posługuje się personelem, podwykonawcami, producentami, dostawcami lub konsultantami nieposługującymi się językiem polskim, zobowiązany jest zapewnić na własny koszt tłumaczenie ustne lub pisemne w zakresie niezbędnym do sprawnego prowadzenia projektu i skutecznego udziału Zamawiającego w czynnościach projektowych, technicznych, odbiorowych i eksploatacyjnych.

e) Brak zapewnienia dokumentacji, komunikacji, tłumaczeń albo obsługi projektu w języku polskim nie może stanowić podstawy do wydłużenia terminów realizacji, ograniczenia odpowiedzialności Generalnego Wykonawcy ani zgłaszania roszczeń wobec Zamawiającego.

25) Generalny Wykonawca zobowiązany jest przedłożyć Zamawiającemu do akceptacji dokumentację projektową przed rozpoczęciem robót, dostaw, instalacji, montażu, konfiguracji lub wdrożenia objętego daną dokumentacją. Rozpoczęcie realizacji danego zakresu bez wymaganej akceptacji dokumentacji projektowej odbywa się na ryzyko Generalnego Wykonawcy i nie może stanowić podstawy do roszczeń wobec Zamawiającego.

26) Akceptacja dokumentacji projektowej przez Zamawiającego nie zwalnia Generalnego Wykonawcy z odpowiedzialności za kompletność, poprawność, zgodność z przepisami, zgodność z normami, zgodność z PFU, zgodność z warunkami zarządców, bezpieczeństwo, funkcjonalność, interoperacyjność, cyberbezpieczeństwo, trwałość i skuteczność zaprojektowanego rozwiązania.

27) Generalny Wykonawca zobowiązany jest prowadzić projektowanie w sposób iteracyjny i uzgodnieniowy, z uwzględnieniem uwag Zamawiającego, wyników wizji lokalnych, wyników analiz technicznych, wymagań zarządców obiektów, wymagań formalnoprawnych oraz wyników uzgodnień branżowych. Każda istotna zmiana przyjętych założeń projektowych musi zostać udokumentowana, uzasadniona i zatwierdzona przez Zamawiającego przed jej wdrożeniem.

28) W przypadku gdy osiągnięcie wymaganej funkcjonalności systemu RIS wymaga wykonania dodatkowych czynności projektowych, analiz, obliczeń, pomiarów, ekspertyz,

uzgodnień, projektów branżowych, projektów zamiennych albo dokumentacji pomocniczej niewymienionej wprost w PFU, Generalny Wykonawca zobowiązany jest wykonać te czynności w ramach wynagrodzenia umownego, bez prawa do dodatkowego wynagrodzenia, o ile są one niezbędne do prawidłowej realizacji przedmiotu zamówienia.

1.2.3. Wymagania w stosunku do systemu łączności radiowej VHF/AIS/DGNSS

Generalny Wykonawca zobowiązany jest zaprojektować i wykonać system łączności radiowej VHF/AIS/DGNSS zgodnie z wymaganiami PFU, dokumentem „PLAN ŁĄCZNOŚCI RADIOWEJ VHF/AIS”, obowiązującymi przepisami prawa, wymaganiami dotyczącymi radiokomunikacji, wymaganiami dotyczącymi usług RIS, wymaganiami właściwych organów administracji, warunkami zarządców nieruchomości i obiektów oraz zasadami należytej praktyki inżynierskiej.

System musi zapewniać realizację funkcji wymaganych dla podsystemu łączności radiowej RIS, w szczególności:

1) odbiór, przetwarzanie i przekazywanie danych AIS z lokalizacji terenowych do systemów centralnych RIS;
2) obsługę stacji brzegowych AIS, w tym pracy podstawowej i zapasowej, jeżeli wynika to z przyjętej architektury;
3) dystrybucję poprawek DGNSS w zakresie wymaganym dla systemu RIS;
4) prowadzenie łączności głosowej VHF z poziomu Centrum RIS;
5) wybór, obsługę i nadzór nad stacjami VHF przez operatorów;
6) prezentację informacji o aktywnej stacji, kanale pracy, stanie urządzeń, alarmach i zdarzeniach;
7) rejestrację zdarzeń, alarmów oraz informacji wymaganych przez przyjęty model eksploatacyjny;
8) centralny nadzór techniczny nad pracą urządzeń, transmisją danych i zasilaniem;
9) współpracę z istniejącymi oraz nowymi komponentami systemu RIS;
10) ciągłość działania i możliwość pracy awaryjnej na poziomie wynikającym z przyjętej architektury technicznej.

Rozwiązanie musi zostać zaprojektowane w sposób zapewniający interoperacyjność, bezpieczeństwo, niezawodność, skalowalność i możliwość eksploatacji w całym okresie życia systemu. Generalny Wykonawca zobowiązany jest zapewnić, aby zastosowane komponenty sprzętowe i programowe były kompatybilne z docelową architekturą RIS oraz umożliwiały integrację z systemami centralnymi, systemami operatorskimi, systemami nadzoru, systemami rejestracji i innymi podsystemami objętymi przedmiotem zamówienia.

Projekt podsystemu musi uwzględniać wymagania dotyczące pokrycia radiowego, zasięgu użytecznego, ograniczenia zakłóceń, parametrów torów antenowych, separacji anten, konfiguracji stacji, doboru urządzeń, zasilania podstawowego i rezerwowego, transmisji danych,

monitoringu technicznego, ochrony przepięciowej, uziemienia, ochrony odgromowej, warunków montażu oraz dostępności serwisowej.

Generalny Wykonawca zobowiązany jest wykonać lub zaktualizować analizy, obliczenia, pomiary i weryfikacje niezbędne do potwierdzenia, że projektowane rozwiązanie spełnia wymagania funkcjonalne i techniczne systemu RIS. W szczególności dotyczy to analiz propagacyjnych, oceny zasięgów stacji AIS i VHF, oceny wpływu lokalizacji oraz wysokości zawieszenia anten na jakość pracy systemu, a także potwierdzenia braku negatywnego wpływu projektowanych instalacji na ludzi, inne systemy i istniejącą infrastrukturę.

Generalny Wykonawca zobowiązany jest zapewnić integrację podsystemu VHF/AIS/DGNSS z systemem RIS i systemami centralnymi. Integracja musi obejmować co najmniej przekazywanie danych AIS, obsługę funkcji DGNSS, obsługę zdalnej łączności VHF, przekazywanie alarmów technicznych, rejestrację zdarzeń oraz udostępnianie informacji diagnostycznych. Integracja musi zostać wykonana bez pogorszenia pracy istniejących komponentów systemu RIS.

Generalny Wykonawca zobowiązany jest zapewnić zasilanie podstawowe i rezerwowe dla lokalizacji objętych podsystemem VHF/AIS/DGNSS. Dobór zasilania rezerwowego musi wynikać z rzeczywistego poboru mocy urządzeń, krytyczności lokalizacji, wymagań ciągłości działania, warunków lokalizacyjnych i dostępności serwisowej. Każda lokalizacja musi być objęta transmisją danych zapewniającą komunikację z Centrum RIS oraz nadzorem technicznym obejmującym co najmniej stan urządzeń, stan transmisji, stan zasilania, alarmy techniczne i zdarzenia eksploatacyjne.

Generalny Wykonawca zobowiązany jest przygotować, skompletować i przeprowadzić w imieniu Zamawiającego dokumentację oraz postępowania niezbędne do uzyskania wymaganych pozwoleń radiowych dla nowych stacji AIS i VHF, jeżeli obowiązek ich uzyskania wynika z przepisów prawa. Uruchomienie emisji radiowej może nastąpić wyłącznie po uzyskaniu właściwych decyzji administracyjnych albo w zakresie dopuszczonym przepisami prawa, decyzjami lub uzgodnieniami właściwego organu.

Generalny Wykonawca zobowiązany jest opracować dokumentację techniczną, konfiguracyjną, odbiorową i eksploatacyjną dla wszystkich elementów podsystemu VHF/AIS/DGNSS objętych zakresem zamówienia. Dokumentacja musi umożliwiać Zamawiającemu identyfikację zastosowanych rozwiązań, lokalizacji, konfiguracji, urządzeń, interfejsów, parametrów pracy, zasad eksploatacji, zasad testowania, zasad utrzymania, zasad diagnostyki i zasad odtwarzania pracy po awarii.

Odbiór podsystemu VHF/AIS/DGNSS musi zostać poprzedzony testami potwierdzającymi spełnienie wymagań funkcjonalnych, technicznych, integracyjnych, zasięgowych, eksploatacyjnych i bezpieczeństwa. Testy muszą obejmować co najmniej pracę warstwy AIS, dystrybucję poprawek DGNSS, obsługę łączności głosowej VHF, obsługę operatorską, nadzór techniczny, alarmowanie, rejestrację zdarzeń, pracę z zasilania rezerwowego, utratę i powrót transmisji danych oraz integrację z systemami centralnymi RIS. Wyniki testów muszą zostać udokumentowane w protokołach odbiorowych.

Szczegółowe wymagania dotyczące lokalizacji, konfiguracji technicznej, funkcji, parametrów radiowych, analiz propagacyjnych, instalacji antenowych, zasilania, transmisji danych, nadzoru technicznego, pozwoleń radiowych, dokumentacji i testów

określa dokument „PLAN ŁĄCZNOŚCI RADIOWEJ VHF/AIS”. W przypadku rozbieżności pomiędzy ogólnym opisem zawartym w PFU a szczegółowymi wymaganiami dokumentu branżowego Generalny Wykonawca zobowiązany jest przyjąć wymaganie zapewniające wyższy poziom funkcjonalności, bezpieczeństwa, niezawodności, interoperacyjności i zgodności z celem projektu, po uzgodnieniu z Zamawiającym.

1.2.4. Wymagania w stosunku do systemu monitoringu wizyjnego (CCTV)

Generalny Wykonawca zobowiązany jest zaprojektować i wykonać system monitoringu wizyjnego CCTV zgodnie z wymaganiami PFU, dokumentem „PLAN SYSTEMU MONITORINGU WIZYJNEGO (CCTV)”, obowiązującymi przepisami prawa, wymaganiami dotyczącymi ochrony danych osobowych i prywatności, wymaganiami cyberbezpieczeństwa, wymaganiami zarządców obiektów oraz zasadami należytej praktyki inżynierskiej.

System CCTV musi zapewniać realizację funkcji wymaganych dla podsystemu monitoringu wizyjnego RIS, w szczególności:

1) obserwację Odrzańskiej Drogi Wodnej oraz miejsc istotnych dla bezpieczeństwa ruchu żeglugowego;
2) obserwację wybranych obiektów infrastruktury technicznej RIS;
3) podgląd obrazu na żywo przez uprawnionych użytkowników;
4) rejestrację i odtwarzanie obrazu;
5) obsługę kamer stałych i kamer PTZ;
6) organizację kamer w widokach, mapach, układach operatorskich i grupach funkcjonalnych;
7) udostępnianie obrazu innym komponentom systemu RIS;
8) kontrolę dostępu i uprawnień użytkowników;
9) obsługę zdarzeń, alarmów i komunikatów technicznych;
10) monitoring techniczny działania kamer, urządzeń, usług, rejestracji i transmisji;
11) eksport materiału wideo i dokumentowanie zdarzeń;
12) zapewnienie ciągłości działania funkcji CCTV na poziomie wynikającym z przyjętej architektury technicznej.

Rozwiązanie musi zostać zaprojektowane w sposób zapewniający interoperacyjność, bezpieczeństwo, skalowalność, dostępność, możliwość utrzymania oraz możliwość dalszej rozbudowy. Generalny Wykonawca zobowiązany jest zapewnić, aby zastosowane komponenty sprzętowe i programowe były kompatybilne z docelową architekturą RIS oraz umożliwiały integrację z systemami centralnymi, systemami operatorskimi, systemami transmisji danych, systemami monitoringu technicznego i mechanizmami zarządzania uprawnieniami.

Projekt systemu CCTV musi uwzględniać wymagania dotyczące jakości obrazu, pola widzenia, kierunku obserwacji, widoczności obszaru referencyjnego, parametrów kamer, parametrów transmisji strumieni wideo, retencji i archiwizacji nagrań, ochrony prywatności, masek prywatności, uprawnień użytkowników, monitoringu technicznego, odporności środowiskowej, bezpieczeństwa fizycznego, zasilania, uziemienia, ochrony przepięciowej, prowadzenia okablowania, montażu oraz dostępności serwisowej.

Generalny Wykonawca zobowiązany jest zaprojektować punkty kamerowe w sposób wynikający z funkcji obserwacyjnej danego punktu. Dla każdego punktu należy określić co najmniej cel obserwacji, wymagany obszar widoczności, kierunki obserwacji, typ i liczbę kamer, sposób montażu, sposób zasilania, sposób transmisji danych, wymagania ochrony prywatności, dostęp serwisowy, ograniczenia lokalizacyjne oraz warunki odbioru widoczności.

System CCTV musi zapewniać centralne zarządzanie obrazem, nagraniami, widokami, użytkownikami, uprawnieniami, zdarzeniami i alarmami. Operatorzy oraz administratorzy systemu nie mogą być zmuszani do korzystania z rozproszonych, niespójnych narzędzi obsługi dla poszczególnych grup kamer, chyba że wynika to z uzasadnionych wymagań bezpieczeństwa, separacji środowisk lub organizacji pracy zaakceptowanych przez Zamawiającego.

System CCTV musi zapewniać możliwość rejestracji, retencji, odtwarzania i eksportu nagrań zgodnie z wymaganiami określonymi w dokumencie branżowym. Eksport materiału musi być realizowany w sposób kontrolowany, audytowalny i możliwy do wykorzystania poza środowiskiem produkcyjnym CCTV, bez naruszenia integralności materiału, zasad bezpieczeństwa oraz zasad ochrony prywatności.

Generalny Wykonawca zobowiązany jest zapewnić integrację systemu CCTV z systemem RIS. Integracja musi obejmować co najmniej udostępnianie obrazu uprawnionym komponentom systemu RIS, powiązanie kamer z lokalizacjami i widokami sytuacyjnymi, kontrolę dostępu do obrazu, monitorowanie dostępności strumieni oraz obsługę wymagań dotyczących bezpiecznego udostępniania obrazu. Integracja nie może pogarszać wydajności, bezpieczeństwa ani dostępności systemu RIS.

Generalny Wykonawca zobowiązany jest zapewnić ochronę prywatności w obrazie z kamer. Projekt musi uwzględniać identyfikację obszarów wymagających maskowania, wdrożenie masek prywatności, kontrolę ich działania w podglądzie, nagraniu, odtwarzaniu i eksporcie oraz zabezpieczenie przed nieuprawnioną zmianą konfiguracji masek. Wymagania ochrony prywatności muszą być uwzględniane już na etapie projektowania pola widzenia kamer.

Generalny Wykonawca zobowiązany jest zapewnić monitoring techniczny podsystemu CCTV. Monitoring musi obejmować co najmniej dostępność kamer, dostępność strumieni wideo, stan rejestracji, stan usług, stan urządzeń, stan transmisji danych, stan zasilania, alarmy techniczne oraz zdarzenia utrzymaniowe. Informacje diagnostyczne muszą być dostępne dla uprawnionych administratorów i służb utrzymaniowych Zamawiającego.

System CCTV musi zostać zaprojektowany w sposób zapewniający możliwość pracy w warunkach awaryjnych oraz możliwość weryfikacji odporności rozwiązania. Wymagania te obejmują w szczególności utratę kamery, utratę węzła rejestracji, przejęcie pracy przez drugi węzeł, odtworzenie nagrania po awarii, odtwarzanie po okresie retencji, poprawność uprawnień, eksport materiału oraz działanie monitoringu technicznego i alarmów.

Generalny Wykonawca zobowiązany jest opracować dokumentację projektową, wykonawczą, powykonawczą, konfiguracyjną, odbiorową i eksploatacyjną dla wszystkich elementów systemu CCTV objętych zakresem zamówienia. Dokumentacja musi umożliwiać Zamawiającemu identyfikację lokalizacji, urządzeń, konfiguracji, widoków, masek prywatności, uprawnień, reguł integracyjnych, parametrów transmisji, parametrów retencji, procedur eksploatacyjnych, procedur testowych i procedur utrzymaniowych.

Odbiór systemu CCTV musi zostać poprzedzony testami potwierdzającymi spełnienie wymagań funkcjonalnych, technicznych, integracyjnych, bezpieczeństwa, transmisyjnych, eksploatacyjnych i odbiorowych. Testy muszą obejmować co najmniej podgląd obrazu na żywo, rejestrację, odtwarzanie, retencję, eksport, obsługę kamer PTZ, widoki operatorskie, mapy i lokalizacje, kontrolę uprawnień, działanie masek prywatności, integrację z RIS, monitoring techniczny, alarmowanie oraz scenariusze awaryjne. Wyniki testów muszą zostać udokumentowane w protokołach odbiorowych.

Szczegółowe wymagania dotyczące lokalizacji, widoczności, parametrów kamer, platformy rejestracji, stacji klienckich, środowiska prezentacji obrazu, transmisji strumieni wideo, retencji, archiwizacji, integracji, bezpieczeństwa, ochrony prywatności, instalacji kablowych, instalacji montażowych, narzędzi obsługi, systemu transmisyjnego, dokumentacji i testów określa dokument „PLAN SYSTEMU MONITORINGU WIZYJNEGO (CCTV)”. W przypadku rozbieżności pomiędzy ogólnym opisem zawartym w PFU a szczegółowymi wymaganiami dokumentu branżowego Generalny Wykonawca zobowiązany jest przyjąć wymaganie zapewniające wyższy poziom funkcjonalności, bezpieczeństwa, niezawodności, interoperacyjności, ochrony prywatności i zgodności z celem projektu, po uzgodnieniu z Zamawiającym.

1.2.5. Wymagania w stosunku do sieci połączeń transmisyjnych

Generalny Wykonawca zobowiązany jest zaprojektować i wykonać sieć połączeń transmisyjnych zgodnie z wymaganiami PFU, dokumentem „PLAN POŁĄCZEŃ TRANSMISYJNYCH”, obowiązującymi przepisami prawa, wymaganiami dotyczącymi cyberbezpieczeństwa, wymaganiami dotyczącymi infrastruktury telekomunikacyjnej, wymaganiami producentów urządzeń, warunkami operatorów telekomunikacyjnych, warunkami zarządców obiektów oraz zasadami należytej praktyki inżynierskiej.

Sieć połączeń transmisyjnych musi zapewniać realizację funkcji wymaganych dla systemu RIS, w szczególności:

1) bezpieczną transmisję danych pomiędzy lokalizacjami terenowymi a Centrum RIS;
2) transmisję strumieni wideo z kamer CCTV;
3) transmisję danych AIS, VHF, DGNSS, danych telemetrycznych, danych hydrologicznych i meteorologicznych;
4) transmisję sygnałów sterowania, danych diagnostycznych, alarmów i informacji utrzymaniowych;
5) komunikację z systemami centralnymi, serwerownią główną i serwerownią zapasową;
6) obsługę monitoringu technicznego i zdalnego utrzymania;

7) separację ruchu poszczególnych klas urządzeń i usług;
8) priorytetyzację ruchu krytycznego dla działania systemu RIS;
9) pracę w trybie podstawowym i zapasowym;
10) możliwość rozbudowy i dalszej integracji z kolejnymi komponentami systemu RIS.

Rozwiązanie musi zostać zaprojektowane w sposób zapewniający kompatybilność z istniejącą siecią transmisji danych RIS. Generalny Wykonawca zobowiązany jest uwzględnić istniejącą architekturę logiczną, model komunikacji pomiędzy lokalizacjami terenowymi a Centrum RIS, segmentację sieci, adresację IP, nazewnictwo urządzeń, polityki bezpieczeństwa, mechanizmy routingu, mechanizmy VPN, system monitorowania oraz zasady wykonywania i przechowywania kopii konfiguracji urządzeń sieciowych.

Projekt sieci transmisji danych musi być oparty na rzeczywistym zapotrzebowaniu transmisyjnym urządzeń i usług systemu RIS. Generalny Wykonawca zobowiązany jest określić wymagane przepustowości dla każdej lokalizacji i każdej klasy ruchu, z uwzględnieniem liczby kamer, parametrów strumieni wideo, liczby sensorów, liczby urządzeń VHF/AIS/DGNSS, danych telemetrycznych, ruchu administracyjnego, ruchu monitoringu technicznego, ruchu bezpieczeństwa oraz wymaganej rezerwy rozwojowej.

Generalny Wykonawca zobowiązany jest zapewnić redundancję torów dostępowych dla lokalizacji objętych zakresem zamówienia, adekwatnie do ich znaczenia dla działania systemu RIS. Redundancja może być realizowana z wykorzystaniem różnych technologii transmisyjnych, w tym łączy operatorskich, łączy komórkowych różnych operatorów, łączy radioliniowych, łączy przewodowych, światłowodowych albo innych rozwiązań zaakceptowanych przez Zamawiającego. Dobór technologii musi wynikać z analizy technicznej, dostępności usług, warunków terenowych, wymagań przepustowościowych, wymagań bezpieczeństwa i wymagań ciągłości działania.

Sieć transmisyjna musi zapewniać bezpieczeństwo transmisji danych. Wymagane jest co najmniej stosowanie separacji ruchu, segmentacji sieci, kontroli dostępu, szyfrowania transmisji, bezpiecznych tuneli VPN, reguł zapór sieciowych, kontroli ruchu pomiędzy strefami, ograniczenia usług administracyjnych, rejestrowania zdarzeń, monitoringu stanu połączeń oraz zabezpieczenia urządzeń brzegowych przed nieuprawnionym dostępem.

Generalny Wykonawca zobowiązany jest zapewnić mechanizmy jakości usług i priorytetyzacji ruchu. Ruch krytyczny dla działania systemu RIS, w szczególności ruch związany z funkcjami VHF/AIS/DGNSS, alarmowaniem, sterowaniem, monitoringiem technicznym oraz usługami operatorskimi, musi być traktowany priorytetowo wobec ruchu pomocniczego. Transmisja strumieni wideo musi zostać zaprojektowana w sposób zapewniający wymagany poziom jakości obrazu bez destabilizacji pracy pozostałych usług systemu RIS.

Generalny Wykonawca zobowiązany jest zapewnić monitoring, diagnostykę i zdalne utrzymanie sieci transmisji danych. Monitoring musi obejmować co najmniej stan urządzeń brzegowych, dostępność łączy podstawowych i zapasowych, parametry jakościowe połączeń, wykorzystanie przepustowości, zdarzenia awaryjne, stan tuneli VPN, stan przełączenia awaryjnego, stan zasilania urządzeń transmisyjnych oraz alarmy techniczne. Informacje diagnostyczne muszą być dostępne dla uprawnionych administratorów i służb utrzymaniowych Zamawiającego.

Projekt sieci transmisji danych musi uwzględniać możliwość skalowania systemu. Rozwiązanie musi umożliwiać dołączenie kolejnych lokalizacji, zwiększenie liczby urządzeń, zwiększenie liczby strumieni wideo, uruchomienie dodatkowych usług cyfrowych, zmianę parametrów transmisyjnych oraz rozbudowę warstwy monitoringu bez konieczności przebudowy podstawowej architektury sieci.

Generalny Wykonawca zobowiązany jest opracować schemat sieci transmisyjnej w wersji projektowej i powykonawczej. Schemat musi obejmować co najmniej wszystkie lokalizacje objęte rozbudową, technologie transmisji dla każdej lokalizacji, tory podstawowe i zapasowe, centralne koncentratory transmisji, lokalne urządzenia brzegowe, połączenia z istniejącą siecią RIS, relacje logiczne tuneli transmisyjnych, segmenty sieciowe, strefy bezpieczeństwa, punkty monitorowania i zarządzania, elementy redundantne oraz lokalizacje wymagające indywidualnego rozwiązania projektowego.

Odbiór sieci połączeń transmisyjnych musi zostać poprzedzony testami potwierdzającymi spełnienie wymagań funkcjonalnych, technicznych, przepustowościowych, bezpieczeństwa, niezawodnościowych, integracyjnych i eksploatacyjnych. Testy muszą obejmować co najmniej dostępność łączy podstawowych i zapasowych, uzyskiwane przepustowości, opóźnienia, stabilność połączeń, działanie tuneli VPN, przełączenie awaryjne, powrót do toru podstawowego, separację ruchu, działanie reguł bezpieczeństwa, monitoring techniczny, alarmowanie oraz komunikację z systemami centralnymi RIS. Wyniki testów muszą zostać udokumentowane w protokołach odbiorowych.

Generalny Wykonawca zobowiązany jest opracować dokumentację projektową, wykonawczą, powykonawczą, konfiguracyjną, odbiorową i eksploatacyjną dla wszystkich elementów sieci transmisji danych objętych zakresem zamówienia. Dokumentacja musi umożliwiać Zamawiającemu identyfikację lokalizacji, technologii transmisji, urządzeń, konfiguracji, adresacji, nazw urządzeń, segmentów sieci, reguł bezpieczeństwa, torów podstawowych i zapasowych, procedur przełączenia awaryjnego, procedur odtworzeniowych, procedur utrzymaniowych i procedur testowych.

Szczegółowe wymagania dotyczące lokalizacji, przepustowości, relacji transmisyjnych, technologii transmisji, bezpieczeństwa, segmentacji, redundancji, QoS, monitoringu, diagnostyki, skalowalności, schematu sieci, wykazu łączy, dokumentacji i testów określa dokument „PLAN POŁĄCZEŃ TRANSMISYJNYCH”. W przypadku rozbieżności pomiędzy ogólnym opisem zawartym w PFU a szczegółowymi wymaganiami dokumentu branżowego Generalny Wykonawca zobowiązany jest przyjąć wymaganie zapewniające wyższy poziom funkcjonalności, bezpieczeństwa, niezawodności, interoperacyjności, dostępności i zgodności z celem projektu, po uzgodnieniu z Zamawiającym.

1.2.6. Wymagania dla czujników hydrologicznych i danych pomiarowych

Generalny Wykonawca zobowiązany jest zaprojektować, dostarczyć, zamontować, skonfigurować, uruchomić, zintegrować, przetestować i przekazać do eksploatacji czujniki hydrologiczne oraz powiązane z nimi elementy pomiarowe, transmisyjne, zasilające, montażowe, diagnostyczne i dokumentacyjne zgodnie z PFU, dokumentacją projektową, wymaganiami

Zamawiającego, warunkami zarządców obiektów, obowiązującymi przepisami prawa, właściwymi normami i dobrą praktyką inżynierską.

Czujniki hydrologiczne muszą zapewniać bieżący, automatyczny pomiar stanu wody w lokalizacjach wskazanych w PFU. Preferowaną metodą pomiaru jest metoda bezkontaktowa, teledetekcyjna, w szczególności metoda radarowa lub równoważna, umożliwiająca ciągły pomiar poziomu lustra wody bez konieczności ingerencji urządzenia pomiarowego w nurt rzeki. Dopuszczone rozwiązanie musi być odporne na warunki środowiskowe występujące na Odrzańskiej Drodze Wodnej, w tym zmienne temperatury, wilgotność, opady, oblodzenie, wiatr, mgłę, zapylenie, oddziaływanie promieniowania słonecznego oraz inne czynniki typowe dla instalacji zewnętrznych na obiektach mostowych.

W każdej lokalizacji należy zapewnić redundantny pomiar stanu wody, realizowany przez co najmniej dwa niezależne czujniki pomiarowe albo rozwiązanie równoważne funkcjonalnie. System musi umożliwiać porównywanie odczytów z torów pomiarowych, wykrywanie rozbieżności pomiarowych, sygnalizowanie błędu, wskazanie toru pomiarowego niespełniającego warunków poprawności oraz utrzymanie funkcji pomiarowej w przypadku awarii pojedynczego czujnika lub pojedynczego toru pomiarowego.

Urządzenia pomiarowe muszą umożliwiać co najmniej:

1) bieżący pomiar stanu wody;
2) konfigurację interwałów próbkowania;
3) uśrednianie wyników pomiarów;
4) lokalny albo zdalny odczyt parametrów pracy urządzenia;
5) lokalny albo zdalny odczyt błędów i stanów diagnostycznych;
6) automatyczne generowanie alarmów i powiadomień o błędach;
7) transmisję danych pomiarowych do Centrum RIS;
8) przekazywanie danych w standardowych formatach i przez interfejsy zgodne z projektowaną architekturą systemu RIS;
9) programową kalibrację i korektę wskazań;
10) integrację z rozwiązaniami aplikacyjnymi systemu RIS służącymi do prezentacji, przetwarzania, weryfikacji, publikacji lub dalszego udostępniania danych pomiarowych.

Dane pomiarowe z poszczególnych lokalizacji muszą być przekazywane do systemu RIS w sposób umożliwiający ich identyfikację, walidację, prezentację, archiwizację, diagnostykę oraz wykorzystanie przez inne komponenty systemu. Każdy rekord danych pomiarowych powinien zawierać co najmniej identyfikator lokalizacji, identyfikator toru pomiarowego lub czujnika, znacznik czasu, wartość pomiarową, jednostkę, status jakości danych, status urządzenia oraz informację o ewentualnym błędzie, ostrzeżeniu albo trybie pracy.

W każdej lokalizacji czujników hydrologicznych Generalny Wykonawca zobowiązany jest zapewnić lokalny komponent akwizycji, przetwarzania, buforowania i transmisji danych pomiarowych, umożliwiający obsługę zastosowanych czujników, rejestrację odczytów, kontrolę

poprawności danych, przekazywanie danych do Centrum RIS oraz zachowanie ciągłości rejestracji pomiarów w przypadku czasowej utraty połączenia transmisyjnego z Centrum RIS.

Lokalny komponent akwizycji danych musi umożliwiać komunikację z czujnikami hydrologicznymi i urządzeniami towarzyszącymi z wykorzystaniem interfejsów oraz protokołów właściwych dla zastosowanych urządzeń pomiarowych, w szczególności wyjść cyfrowych SDI-12, RS-232, RS-485, RS-422 oraz protokołów transmisji ASCII, SDI-12, NMEA i Modbus RTU, jeżeli są one wymagane do obsługi wybranego rozwiązania technicznego. Dopuszcza się zastosowanie innych standardowych interfejsów lub protokołów, pod warunkiem zapewnienia pełnej interoperacyjności, dokumentacji, możliwości utrzymania oraz akceptacji rozwiązania przez Zamawiającego.

Komponent lokalny musi realizować co najmniej następujące funkcje:

1) cykliczny odczyt danych z czujników hydrologicznych zgodnie z konfigurowalnym interwałem pomiarowym;
2) odbiór danych diagnostycznych, statusów pracy, błędów i alarmów generowanych przez czujniki oraz urządzenia towarzyszące;
3) wstępne przetwarzanie danych pomiarowych, w tym co najmniej przypisanie identyfikatora lokalizacji, identyfikatora czujnika albo toru pomiarowego, znacznika czasu, jednostki pomiarowej oraz statusu jakości danych;
4) obsługę redundantnych torów pomiarowych, w tym porównywanie odczytów z dwóch czujników, wykrywanie rozbieżności i generowanie alarmów;
5) lokalną rejestrację danych pomiarowych, diagnostycznych i alarmowych;
6) przekazywanie danych do Centrum RIS w trybie bieżącym, jeżeli połączenie transmisyjne jest dostępne;
7) buforowanie danych w przypadku utraty połączenia transmisyjnego z Centrum RIS;
8) automatyczne przekazanie danych zaległych do Centrum RIS po wznowieniu połączenia transmisyjnego;
9) zabezpieczenie danych przed utratą, nieuprawnioną modyfikacją i nadpisaniem przed ich skutecznym przekazaniem do Centrum RIS;
10) rejestrację informacji o przerwach w komunikacji, czasie rozpoczęcia i zakończenia przerwy, liczbie zgromadzonych rekordów oraz statusie ich późniejszego przekazania do Centrum RIS.

Lokalny komponent akwizycji danych musi zapewniać buforowanie danych przez okres nie krótszy niż 7 dni pracy danej lokalizacji przy docelowej częstotliwości pomiaru i raportowania, chyba że dokumentacja projektowa, analiza ryzyka albo wymagania Zamawiającego wykażą konieczność przyjęcia dłuższego okresu buforowania. Pojemność bufora musi obejmować dane pomiarowe, dane diagnostyczne, alarmy, zdarzenia komunikacyjne oraz informacje o statusie urządzeń.

Dane zgromadzone lokalnie w czasie utraty połączenia transmisyjnego muszą być oznaczane rzeczywistym czasem wykonania pomiaru, a nie wyłącznie czasem późniejszego przekazania do

Centrum RIS. Po wznowieniu transmisji system musi umożliwiać odróżnienie danych bieżących od danych zaległych oraz zachować ich kolejność, integralność i identyfikowalność.

Komponent lokalny musi działać autonomicznie w zakresie niezbędnym do kontynuowania odczytu i rejestracji danych z czujników hydrologicznych bez udziału Centrum RIS. Utrata połączenia z Centrum RIS nie może powodować zatrzymania pomiarów, utraty konfiguracji, utraty danych już zgromadzonych ani braku możliwości dalszego lokalnego rejestrowania odczytów.

Generalny Wykonawca zobowiązany jest zapewnić możliwość zdalnej konfiguracji, diagnostyki, aktualizacji i nadzoru nad komponentem lokalnym przez uprawniony personel Zamawiającego albo służby utrzymaniowe działające na jego rzecz. Funkcje administracyjne muszą być zabezpieczone przed nieuprawnionym dostępem, a zmiany konfiguracji muszą być rejestrowane i możliwe do odtworzenia.

Komponent lokalny musi być objęty monitoringiem technicznym systemu RIS. Monitoring musi obejmować co najmniej dostępność komponentu, status komunikacji z czujnikami, status komunikacji z Centrum RIS, status zasilania, stan bufora danych, liczbę rekordów oczekujących na wysłanie, błędy odczytu, błędy transmisji, błędy zapisu lokalnego, alarm przepełnienia bufora oraz alarm braku skutecznego przekazania danych po wznowieniu transmisji.

W ramach odbioru czujników hydrologicznych Generalny Wykonawca zobowiązany jest przeprowadzić test utraty i powrotu połączenia transmisyjnego z Centrum RIS. Test musi potwierdzić, że lokalny komponent kontynuuje odczyt danych z czujników, zapisuje dane lokalnie, prawidłowo oznacza czas pomiaru, sygnalizuje utratę komunikacji, a po przywróceniu połączenia przekazuje dane zaległe do Centrum RIS bez utraty, duplikacji i naruszenia integralności danych.

Zamawiający wymaga, aby dane pomiarowe udostępniane do publikacji w innych komponentach systemu RIS albo przekazywane do interesariuszy zewnętrznych mogły być korygowane o wartość wprowadzaną w dedykowanym rozwiązaniu aplikacyjnym przez uprawnionych pracowników Centrum RIS. Mechanizm korekty musi być rejestrowany, audytowalny i możliwy do odtwórczego zweryfikowania, w tym w zakresie wartości korekty, daty i czasu jej wprowadzenia, użytkownika dokonującego zmiany oraz zakresu obowiązywania korekty.

Punktem odniesienia dla ustalania wartości pomiarowych, kalibracji i kontroli poprawności wskazań ma być Operat Techniczny z pomiarów wodowskazów na obszarze działania rozbudowy systemu RIS na Odrzańskiej Drodze Wodnej. Operat musi określać w szczególności powiązanie punktów wodowskazowych z właściwą osnową geodezyjną, odniesienie wysokościowe, wartości zera wodowskazu, współrzędne punktów, nawiązania wysokościowe, wyniki pomiarów, obliczenia oraz informacje niezbędne do kalibracji, kontroli i późniejszej eksploatacji wodowskazów.

Pomiar musi być odniesiony do właściwego państwowego systemu odniesień przestrzennych oraz do poziomów odniesienia wymaganych dla eksploatacji systemu RIS i prezentacji danych wodowskazowych. Dokumentacja musi umożliwiać jednoznaczne powiązanie wskazań czujnika z zerem wodowskazu oraz z przyjętym układem wysokościowym, w tym z odniesieniem stosowanym w dotychczasowych operatach technicznych Zamawiającego.

Miejsce montażu czujnika musi być dobrane w sposób zapewniający poprawność pomiaru w całym przewidywanym zakresie stanów wody. Czujnik nie może być montowany nad miejscem, w którym przy niskich stanach wody występuje wynurzona podstawa podpory, łacha piasku, element konstrukcyjny, przeszkoda terenowa lub inne zjawisko mogące zafałszować pomiar. Nie dopuszcza się montażu czujników w miejscach lokalnego piętrzenia się wody, turbulencji, zakłóceń przepływu lub w bezpośrednim sąsiedztwie elementów mogących powodować niereprezentatywny odczyt poziomu wody.

Czujnik musi być montowany w obrębie lustra wody, z zachowaniem wolnej przestrzeni pomiarowej pomiędzy czujnikiem a powierzchnią wody. Wiązka pomiarowa musi być skierowana w taki sposób, aby nie była zakłócana przez elementy konstrukcji mostu, podpory, przewody, elementy wyposażenia obiektu, elementy oznakowania, konstrukcje wsporcze, roślinność, osady, pływające przeszkody albo inne obiekty. W przypadku zastosowania pomiaru radarowego należy uwzględnić rozszerzanie się wiązki pomiarowej wraz ze wzrostem odległości od czujnika oraz zapewnić odpowiedni odstęp od pionowych i skośnych elementów konstrukcyjnych.

Montaż czujników i konstrukcji wsporczych musi być wykonany w sposób stabilny, trwały i odporny na drgania, odkształcenia, obciążenia wiatrem, zmiany temperatury oraz oddziaływanie środowiska zewnętrznego. Miejsce montażu nie może przenosić na czujnik drgań mogących wpływać na wynik pomiaru. Konstrukcja montażowa nie może być podatna na odkształcenia powodujące zmianę geometrii pomiaru lub utratę kalibracji. Montaż czujników nie może ograniczać prześwitu pionowego, szerokości żeglownej, światła przęsła, funkcji obiektu mostowego ani bezpieczeństwa żeglugi.

Wysokość montażu czujnika musi być ustalona z uwzględnieniem najwyższych możliwych stanów wody, ryzyka zalania, ryzyka uszkodzenia przez lód, niesione przedmioty, prace utrzymaniowe, ruch na obiekcie mostowym oraz inne czynniki eksploatacyjne. Jednocześnie wysokość montażu musi zapewniać pracę czujnika w zakresie pomiarowym odpowiednim dla danej lokalizacji i umożliwiać uzyskanie wymaganej dokładności pomiaru.

Urządzenia pomiarowe muszą posiadać zakres pomiarowy odpowiedni dla przewidywanych warunków hydrologicznych w danej lokalizacji, przy czym zakres ten nie może być mniejszy niż wymagany dla bezpiecznego pomiaru odległości pomiędzy miejscem montażu a lustrem wody w całym przewidywanym zakresie stanów wody. Dokładność pomiaru musi być odpowiednia dla zastosowań wodowskazowych systemu RIS i nie gorsza niż 0,01 m, o ile szczegółowe uzgodnienia z Zamawiającym albo właściwymi interesariuszami nie wykażą konieczności zastosowania dokładniejszego rozwiązania.

Urządzenia muszą być przystosowane do całorocznej pracy w warunkach zewnętrznych. Wymagany jest stopień ochrony obudowy, odporność klimatyczna, odporność na korozję i odporność mechaniczna adekwatna do miejsca montażu. Urządzenia muszą być zabezpieczone przed skutkami wyładowań atmosferycznych, przepięć, zakłóceń elektromagnetycznych, zaniku zasilania, nieuprawnionej ingerencji oraz przypadkowego uszkodzenia w trakcie eksploatacji lub prac utrzymaniowych prowadzonych na obiekcie.

Czujniki, urządzenia komunikacyjne, zasilające i towarzyszące muszą być zintegrowane z projektowaną siecią teleinformatyczną systemu RIS. Transmisja danych może być realizowana drogą przewodową albo bezprzewodową, z wykorzystaniem technologii zaakceptowanych przez

Zamawiającego, przy zachowaniu wymagań bezpieczeństwa, niezawodności, monitoringu, diagnostyki i kompatybilności z pozostałymi komponentami systemu RIS.

Trasy kablowe dla czujników hydrologicznych, urządzeń zasilania, urządzeń transmisyjnych i urządzeń towarzyszących muszą zostać zaprojektowane i wykonane z uwzględnieniem warunków lokalizacyjnych, konstrukcji obiektu mostowego, wymagań zarządcy obiektu, dostępności serwisowej, ochrony przed uszkodzeniami mechanicznymi, promieniowaniem UV, wilgocią, wodą, oblodzeniem, korozją, drganiami, oddziaływaniem temperatury oraz wpływem prac utrzymaniowych prowadzonych na obiekcie. Trasy kablowe muszą być prowadzone w sposób uporządkowany, trwały, identyfikowalny i możliwy do późniejszej kontroli.

Do wykonania tras kablowych, konstrukcji wsporczych, uchwytów, przepustów, rur osłonowych, koryt, peszli, dławnic, puszek, złączy, opasek, obejm, elementów mocujących i zabezpieczeń należy stosować materiały przeznaczone do pracy w warunkach zewnętrznych, odporne na korozję, promieniowanie UV, wilgoć, zmiany temperatury i oddziaływania mechaniczne. Materiały instalacyjne muszą być dobrane odpowiednio do rodzaju obiektu, miejsca montażu, klasy środowiska, wymagań zarządcy oraz przewidywanego okresu eksploatacji.

Wszystkie przejścia kablowe, przepusty, mocowania i trasy prowadzone na obiektach mostowych muszą być zaprojektowane i wykonane w sposób niepowodujący pogorszenia stanu technicznego obiektu, utraty szczelności, uszkodzenia zabezpieczeń antykorozyjnych, naruszenia elementów konstrukcyjnych ani utrudnienia bieżącej eksploatacji i utrzymania obiektu. W przypadku konieczności ingerencji w elementy obiektu Generalny Wykonawca musi uzyskać wymagane zgody, uzgodnienia, opinie i warunki techniczne właściwego zarządcy.

System musi zapewniać monitoring techniczny czujników hydrologicznych i urządzeń towarzyszących. Monitoring musi obejmować co najmniej dostępność urządzenia, status pracy, status komunikacji, status zasilania, status toru pomiarowego, wystąpienie błędów pomiarowych, rozbieżność pomiędzy torami pomiarowymi, przekroczenie zakresu pracy, utratę komunikacji, awarię urządzenia oraz zdarzenia wymagające interwencji eksploatacyjnej.

Generalny Wykonawca zobowiązany jest zapewnić możliwość kalibracji czujników na podstawie geodezyjnego pomiaru ich wysokości oraz wartości wynikających z Operatu Technicznego z pomiarów wodowskazów. Kalibracja musi być udokumentowana i możliwa do odtworzenia. W ramach dokumentacji należy wskazać wartości kalibracyjne, sposób ich wyznaczenia, datę kalibracji, osobę albo podmiot wykonujący kalibrację oraz wyniki kontroli poprawności wskazań.

W okresie gwarancji i rękojmi Generalny Wykonawca zobowiązany jest zapewnić okresową kontrolę, konserwację, diagnostykę i kalibrację czujników hydrologicznych. Co najmniej raz w roku należy wykonać kontrolę geodezyjną lub niwelację punktów wodowskazowych w zakresie niezbędnym do weryfikacji poprawności wskazań. Kontrola taka musi zostać wykonana również po przebudowie, modernizacji, remoncie, zmianie obciążenia, istotnej ingerencji w obiekt mostowy albo wystąpieniu zdarzenia mogącego mieć wpływ na geometrię pomiaru.

Odbiór czujników hydrologicznych musi obejmować testy funkcjonalne, techniczne, transmisyjne, diagnostyczne, integracyjne i pomiarowe. W szczególności należy potwierdzić poprawność montażu, poprawność geometrii pomiaru, działanie obu torów pomiarowych, poprawność komunikacji z systemem RIS, przekazywanie danych pomiarowych, działanie statusów jakości danych, działanie alarmów, możliwość konfiguracji interwałów próbkowania, możliwość

uśredniania danych, możliwość kalibracji, poprawność odniesienia do wartości wynikających z Operatu Technicznego oraz zgodność dokumentacji powykonawczej ze stanem rzeczywistym.

W ramach odbioru Generalny Wykonawca zobowiązany jest przekazać Zamawiającemu co najmniej: protokoły montażu, protokoły kalibracji, protokoły testów, wykaz nastaw urządzeń, wyniki odczytów testowych, dokumentację powykonawczą lokalizacji, dokumentację tras kablowych, schematy zasilania i transmisji danych, dokumentację konfiguracji, dokumentację integracji z systemem RIS, instrukcje eksploatacyjne oraz Operat Techniczny z pomiarów wodowskazów.

Dane pomiarowe z czujników hydrologicznych muszą być objęte zasadami bezpieczeństwa, integralności, dostępności i rozliczalności właściwymi dla danych eksploatacyjnych systemu RIS. System musi zapewniać ochronę przed nieuprawnioną modyfikacją danych, rejestrowanie zmian konfiguracyjnych, identyfikowalność źródła danych, kontrolę dostępu do funkcji administracyjnych oraz możliwość odtworzenia historii pomiarów, korekt, alarmów i zdarzeń diagnostycznych.

Szczegółowe rozwiązania projektowe, typy urządzeń, miejsca montażu, sposób prowadzenia tras kablowych, sposób zasilania, sposób transmisji danych, parametry konfiguracji, wartości kalibracyjne, powiązanie z osnową geodezyjną, sposób integracji z systemem RIS oraz procedury odbioru i utrzymania muszą zostać określone przez Generalnego Wykonawcę w dokumentacji projektowej, wykonawczej, powykonawczej, konfiguracyjnej, odbiorowej i eksploatacyjnej oraz zaakceptowane przez Zamawiającego.

1.2.7. Wymagania dla czujników meteorologicznych i danych pomiarowych

Generalny Wykonawca zobowiązany jest zaprojektować, dostarczyć, zamontować, skonfigurować, uruchomić, zintegrować, przetestować i przekazać do eksploatacji czujniki meteorologiczne oraz powiązane z nimi elementy pomiarowe, transmisyjne, zasilające, montażowe, diagnostyczne i dokumentacyjne zgodnie z PFU, dokumentacją projektową, wymaganiami Zamawiającego, warunkami zarządców nieruchomości i obiektów, obowiązującymi przepisami prawa, właściwymi normami i dobrą praktyką inżynierską.

Czujniki meteorologiczne muszą zapewniać bieżący, automatyczny pomiar i rejestrację warunków atmosferycznych w lokalizacjach wskazanych w PFU. System pomiarowy musi zapewniać co najmniej pomiar prędkości wiatru, kierunku wiatru, opadów atmosferycznych, ciśnienia barometrycznego, temperatury powietrza oraz wilgotności względnej. Zastosowane rozwiązanie musi umożliwiać transmisję danych do systemu RIS oraz ich dalsze wykorzystanie w usługach informacji hydrometeorologicznej i pozostałych komponentach systemu.

Czujniki meteorologiczne muszą być przystosowane do całorocznej pracy w warunkach zewnętrznych występujących na Odrzańskiej Drodze Wodnej, w szczególności w warunkach niskich i wysokich temperatur, wilgotności, opadów, oblodzenia, silnego wiatru, promieniowania słonecznego, zapylenia, oddziaływania zanieczyszczeń, drgań konstrukcji oraz innych czynników typowych dla instalacji na obiektach wieżowych i hydrotechnicznych. Wymagany jest stopień ochrony obudowy nie niższy niż IP66 albo równoważny poziom ochrony potwierdzający przydatność urządzenia do pracy w warunkach zewnętrznych.

Czujniki meteorologiczne muszą być wykonane w zwartej, odpornej środowiskowo obudowie umożliwiającej montaż na docelowej platformie, w szczególności na wierzchołku obiektu wieżowego na konstrukcji wsporczej przewidzianej w dokumentacji projektowej. Konstrukcja urządzenia oraz sposób montażu muszą ograniczać potrzebę częstych czynności obsługowych i zapewniać możliwość bezpiecznego serwisowania, diagnostyki, wymiany albo kalibracji zgodnie z wymaganiami producenta i Zamawiającego.

Dla zapewnienia reprezentatywności pomiaru czujnik meteorologiczny powinien zostać zlokalizowany na obszarze możliwie odkrytym, z dala od wysokich obiektów, drzew, budynków, ścian, ekranów, urządzeń technicznych, konstrukcji lub innych przesłon mogących wpływać na wynik pomiaru. Lokalizacja i wysokość montażu muszą zostać dobrane w sposób ograniczający zakłócenia pomiaru wiatru, opadu, temperatury i wilgotności, a jednocześnie zapewniający bezpieczeństwo konstrukcji, dostęp serwisowy oraz zgodność z warunkami zarządcy obiektu.

Czujnik meteorologiczny musi posiadać funkcję podgrzewania co najmniej elementów odpowiedzialnych za pomiar prędkości i kierunku wiatru. Funkcja podgrzewania musi umożliwiać ograniczenie wpływu oblodzenia i osadzania się szronu na dostępność oraz poprawność pomiarów. Jeżeli zastosowana technologia pomiaru opadu, wilgotności lub innych parametrów wymaga podgrzewania dodatkowych elementów dla zachowania poprawności pracy, Generalny Wykonawca zobowiązany jest uwzględnić to w dokumentacji projektowej, bilansie energetycznym i konfiguracji zasilania.

Wymagany zakres pracy środowiskowej czujników meteorologicznych nie może być węższy niż od -50°C do +60°C. W przypadku zastosowania urządzeń o innym zakresie pracy Generalny Wykonawca musi wykazać, że zakres ten jest wystarczający dla warunków lokalizacyjnych, klimatycznych i eksploatacyjnych Odrzańskiej Drogi Wodnej oraz nie ograniczy dostępności danych w okresie zimowym i letnim.

Czujnik meteorologiczny musi zapewniać pomiar prędkości wiatru co najmniej w zakresie od 0 do 60 m/s, z rozdzielczością nie gorszą niż 0,1 m/s oraz dokładnością nie gorszą niż 3% dla reprezentatywnych warunków pracy. Pomiar kierunku wiatru musi być realizowany w zakresie 0–360°, z rozdzielczością nie gorszą niż 1° oraz dokładnością odpowiednią dla zastosowań meteorologicznych systemu RIS, nie gorszą niż 5°.

Czujnik meteorologiczny musi zapewniać pomiar opadów atmosferycznych, w tym co najmniej intensywności opadu oraz wartości skumulowanej opadu w okresie pomiarowym. Zakres pomiaru intensywności opadu nie może być mniejszy niż 0–180 mm/h, a dokładność pomiaru opadu nie może być gorsza niż 5% w warunkach określonych przez producenta urządzenia. Jeżeli urządzenie umożliwia rejestrację czasu trwania opadu, intensywności opadu w interwałach krótkookresowych albo detekcję zjawisk gradowych, dane te powinny zostać udostępnione do systemu RIS.

Czujnik meteorologiczny musi zapewniać pomiar ciśnienia barometrycznego w zakresie odpowiednim dla warunków atmosferycznych występujących na obszarze Odrzańskiej Drogi Wodnej, nie węższym niż 600–1100 hPa. Dokładność pomiaru ciśnienia musi być nie gorsza niż 1 hPa w pełnym zakresie pracy środowiskowej urządzenia. Dane ciśnienia powinny być przekazywane w jednostkach powszechnie stosowanych w systemach meteorologicznych, w szczególności hPa albo Pa.

Czujnik meteorologiczny musi zapewniać pomiar temperatury powietrza co najmniej w zakresie od -50°C do +60°C, z dokładnością nie gorszą niż 1°C oraz rozdzielczością umożliwiającą praktyczne wykorzystanie danych w usługach informacji hydrometeorologicznej RIS. Pomiar wilgotności względnej musi być realizowany co najmniej w zakresie 0–100% RH, z dokładnością odpowiednią dla zastosowań meteorologicznych systemu RIS, nie gorszą niż 5% RH w pełnym zakresie pomiarowym.

Urządzenia muszą umożliwiać konfigurację interwałów pomiarowych, uśrednianie danych, określenie wartości chwilowych, średnich, minimalnych i maksymalnych, jeżeli są dostępne dla danego parametru, oraz przekazywanie danych z częstotliwością wynikającą z potrzeb systemu RIS. Minimalna funkcjonalność musi umożliwiać ustawianie interwałów pomiarowych albo raportowania w zakresie umożliwiającym zarówno bieżącą obserwację warunków atmosferycznych, jak i ograniczenie niepotrzebnego obciążenia sieci transmisyjnej.

Urządzenia muszą umożliwiać komunikację poprzez standardowe interfejsy i formaty wymiany danych zgodne z projektowaną siecią teleinformatyczną systemu RIS. Dopuszcza się stosowanie interfejsów przewodowych lub bezprzewodowych oraz protokołów komunikacyjnych powszechnie stosowanych dla urządzeń meteorologicznych i telemetrii, o ile zapewniają one bezpieczną, stabilną i monitorowalną transmisję danych do systemu RIS. Rozwiązanie musi umożliwiać integrację z systemami centralnymi RIS bez konieczności stosowania zamkniętych, niewspieranych albo niedokumentowanych mechanizmów komunikacji.

Każdy rekord danych meteorologicznych przekazywany do systemu RIS powinien zawierać co najmniej identyfikator lokalizacji, identyfikator urządzenia albo toru pomiarowego, znacznik czasu, nazwę parametru, wartość pomiarową, jednostkę, status jakości danych, status urządzenia oraz informację o ewentualnym błędzie, ostrzeżeniu albo trybie pracy. Dane muszą być przekazywane w sposób umożliwiający ich walidację, prezentację, archiwizację, analizę, diagnostykę oraz wykorzystanie przez inne komponenty systemu RIS.

W każdej lokalizacji sensorów meteorologicznych Generalny Wykonawca zobowiązany jest zapewnić lokalny komponent akwizycji, przetwarzania, buforowania i transmisji danych pomiarowych, umożliwiający obsługę zastosowanych sensorów, rejestrację odczytów, kontrolę poprawności danych, przekazywanie danych do Centrum RIS oraz zachowanie ciągłości rejestracji pomiarów w przypadku czasowej utraty połączenia transmisyjnego z Centrum RIS.

Lokalny komponent akwizycji danych musi umożliwiać komunikację z sensorami meteorologicznymi i urządzeniami towarzyszącymi z wykorzystaniem interfejsów oraz protokołów właściwych dla zastosowanych urządzeń pomiarowych, w szczególności wyjść cyfrowych SDI-12, RS-232, RS-485, RS-422 oraz protokołów transmisji ASCII, SDI-12, NMEA i Modbus RTU, jeżeli są one wymagane do obsługi wybranego rozwiązania technicznego. Dopuszcza się zastosowanie innych standardowych interfejsów lub protokołów, pod warunkiem zapewnienia pełnej interoperacyjności, dokumentacji, możliwości utrzymania oraz akceptacji rozwiązania przez Zamawiającego.

Komponent lokalny musi realizować co najmniej następujące funkcje:

1) cykliczny odczyt danych meteorologicznych zgodnie z konfigurowalnym interwałem pomiarowym;

2) odbiór danych diagnostycznych, statusów pracy, błędów i alarmów generowanych przez sensory oraz urządzenia towarzyszące;
3) wstępne przetwarzanie danych pomiarowych, w tym co najmniej przypisanie identyfikatora lokalizacji, identyfikatora sensora, znacznika czasu, nazwy parametru, wartości pomiarowej, jednostki pomiarowej oraz statusu jakości danych;
4) obsługę parametrów meteorologicznych wymaganych w PFU, w szczególności prędkości i kierunku wiatru, opadu, ciśnienia barometrycznego, temperatury powietrza oraz wilgotności względnej;
5) lokalną rejestrację danych pomiarowych, diagnostycznych i alarmowych;
6) przekazywanie danych do Centrum RIS w trybie bieżącym, jeżeli połączenie transmisyjne jest dostępne;
7) buforowanie danych w przypadku utraty połączenia transmisyjnego z Centrum RIS;
8) automatyczne przekazanie danych zaległych do Centrum RIS po wznowieniu połączenia transmisyjnego;
9) zabezpieczenie danych przed utratą, nieuprawnioną modyfikacją i nadpisaniem przed ich skutecznym przekazaniem do Centrum RIS;
10) rejestrację informacji o przerwach w komunikacji, czasie rozpoczęcia i zakończenia przerwy, liczbie zgromadzonych rekordów oraz statusie ich późniejszego przekazania do Centrum RIS.

Lokalny komponent akwizycji danych musi zapewniać buforowanie danych przez okres nie krótszy niż 7 dni pracy danej lokalizacji przy docelowej częstotliwości pomiaru i raportowania, chyba że dokumentacja projektowa, analiza ryzyka albo wymagania Zamawiającego wykażą konieczność przyjęcia dłuższego okresu buforowania. Pojemność bufora musi obejmować dane pomiarowe, dane diagnostyczne, alarmy, zdarzenia komunikacyjne oraz informacje o statusie urządzeń.

Dane zgromadzone lokalnie w czasie utraty połączenia transmisyjnego muszą być oznaczane rzeczywistym czasem wykonania pomiaru, a nie wyłącznie czasem późniejszego przekazania do Centrum RIS. Po wznowieniu transmisji system musi umożliwiać odróżnienie danych bieżących od danych zaległych oraz zachować ich kolejność, integralność i identyfikowalność.

Komponent lokalny musi działać autonomicznie w zakresie niezbędnym do kontynuowania odczytu i rejestracji danych z sensorów meteorologicznych bez udziału Centrum RIS. Utrata połączenia z Centrum RIS nie może powodować zatrzymania pomiarów, utraty konfiguracji, utraty danych już zgromadzonych ani braku możliwości dalszego lokalnego rejestrowania odczytów.

Generalny Wykonawca zobowiązany jest zapewnić możliwość zdalnej konfiguracji, diagnostyki, aktualizacji i nadzoru nad komponentem lokalnym przez uprawniony personel Zamawiającego albo służby utrzymaniowe działające na jego rzecz. Funkcje administracyjne muszą być zabezpieczone przed nieuprawnionym dostępem, a zmiany konfiguracji muszą być rejestrowane i możliwe do odtworzenia.

Komponent lokalny musi być objęty monitoringiem technicznym systemu RIS. Monitoring musi obejmować co najmniej dostępność komponentu, status komunikacji z sensorami, status komunikacji z Centrum RIS, status zasilania, status funkcji podgrzewania, stan bufora danych, liczbę rekordów oczekujących na wysłanie, błędy odczytu, błędy transmisji, błędy zapisu lokalnego, alarm przepełnienia bufora oraz alarm braku skutecznego przekazania danych po wznowieniu transmisji.

W ramach odbioru sensorów meteorologicznych Generalny Wykonawca zobowiązany jest przeprowadzić test utraty i powrotu połączenia transmisyjnego z Centrum RIS. Test musi potwierdzić, że lokalny komponent kontynuuje odczyt danych z sensorów, zapisuje dane lokalnie, prawidłowo oznacza czas pomiaru, sygnalizuje utratę komunikacji, a po przywróceniu połączenia przekazuje dane zaległe do Centrum RIS bez utraty, duplikacji i naruszenia integralności danych.

System musi zapewniać monitoring techniczny czujników meteorologicznych i urządzeń towarzyszących. Monitoring musi obejmować co najmniej dostępność urządzenia, status komunikacji, status zasilania, status funkcji podgrzewania, status torów pomiarowych, przekroczenie zakresu pracy, utratę komunikacji, awarię urządzenia, brak aktualizacji danych, niespójność danych oraz zdarzenia wymagające interwencji eksploatacyjnej.

Czujniki meteorologiczne, urządzenia transmisyjne, urządzenia zasilające i urządzenia towarzyszące muszą zostać zintegrowane z projektowaną siecią teleinformatyczną systemu RIS. Transmisja danych może być realizowana drogą przewodową albo bezprzewodową, z wykorzystaniem technologii zaakceptowanych przez Zamawiającego, przy zachowaniu wymagań bezpieczeństwa, niezawodności, monitoringu, diagnostyki, kompatybilności i skalowalności określonych dla systemu RIS.

Trasy kablowe dla czujników meteorologicznych, urządzeń zasilania, urządzeń transmisyjnych, elementów podgrzewania i urządzeń towarzyszących muszą zostać zaprojektowane i wykonane z uwzględnieniem warunków lokalizacyjnych, rodzaju konstrukcji wsporczej, wymagań zarządcy obiektu, dostępności serwisowej, ochrony przed uszkodzeniami mechanicznymi, promieniowaniem UV, wilgocią, wodą, oblodzeniem, korozją, drganiami, oddziaływaniem temperatury, wiatru oraz wpływem prac utrzymaniowych prowadzonych na obiekcie.

Trasy kablowe muszą być prowadzone w sposób uporządkowany, trwały, identyfikowalny i możliwy do późniejszej kontroli. Należy unikać tras narażonych na bezpośrednie uszkodzenia mechaniczne, niekontrolowane naprężenia, nadmierne zginanie przewodów, spływ wody do urządzeń, gromadzenie się lodu, kolizje z elementami konstrukcyjnymi, elementami instalacji odgromowej, torami antenowymi, instalacjami energetycznymi oraz urządzeniami radiokomunikacyjnymi.

Do wykonania tras kablowych, konstrukcji wsporczych, uchwytów, przepustów, rur osłonowych, koryt, peszli, dławnic, puszek, złączy, opasek, obejm, elementów mocujących i zabezpieczeń należy stosować materiały przeznaczone do pracy w warunkach zewnętrznych, odporne na korozję, promieniowanie UV, wilgoć, zmiany temperatury, drgania, obciążenia wiatrem i oddziaływania mechaniczne. Materiały instalacyjne muszą być dobrane odpowiednio do rodzaju obiektu, miejsca montażu, klasy środowiska, wymagań zarządcy oraz przewidywanego okresu eksploatacji.

Wszystkie przejścia kablowe, przepusty, mocowania i trasy prowadzone na obiektach wieżowych, konstrukcjach wsporczych, obiektach hydrotechnicznych albo innych obiektach

budowlanych muszą być zaprojektowane i wykonane w sposób niepowodujący pogorszenia stanu technicznego obiektu, uszkodzenia zabezpieczeń antykorozyjnych, naruszenia elementów konstrukcyjnych, pogorszenia ochrony odgromowej, powstania zagrożenia porażeniowego ani utrudnienia bieżącej eksploatacji i utrzymania obiektu.

Zasilanie czujników meteorologicznych, urządzeń transmisyjnych i elementów podgrzewania musi zostać dobrane na podstawie rzeczywistego poboru mocy, trybu pracy, wymaganego czasu dostępności, warunków środowiskowych oraz wymagań ciągłości działania. Bilans energetyczny musi uwzględniać pracę czujnika w trybie normalnym, pracę przy zwiększonej częstotliwości pomiarów, pracę funkcji podgrzewania oraz pracę urządzeń towarzyszących, takich jak router, modem, przełącznik, zabezpieczenia, elementy monitoringu technicznego i urządzenia zasilania rezerwowego.

Urządzenia muszą być zabezpieczone przed skutkami wyładowań atmosferycznych, przepięć, zakłóceń elektromagnetycznych, zaniku zasilania, nieuprawnionej ingerencji oraz przypadkowego uszkodzenia w trakcie eksploatacji lub prac utrzymaniowych. Ochrona odgromowa, uziemienie i ochrona przepięciowa muszą być skoordynowane z rozwiązaniami przyjętymi dla obiektu wieżowego, szafy teletechnicznej, torów antenowych, urządzeń transmisyjnych i instalacji zasilającej.

Generalny Wykonawca zobowiązany jest zapewnić możliwość konfiguracji, diagnostyki, aktualizacji, testowania i utrzymania czujników meteorologicznych przez uprawniony personel Zamawiającego albo służby utrzymaniowe działające na jego rzecz. Dostęp do funkcji administracyjnych musi być zabezpieczony przed nieuprawnionym użyciem, a zmiany konfiguracji muszą być dokumentowane i możliwe do odtworzenia.

Dane meteorologiczne muszą być objęte zasadami bezpieczeństwa, integralności, dostępności i rozliczalności właściwymi dla danych eksploatacyjnych systemu RIS. System musi zapewniać ochronę przed nieuprawnioną modyfikacją danych, rejestrowanie zmian konfiguracyjnych, identyfikowalność źródła danych, kontrolę dostępu do funkcji administracyjnych oraz możliwość odtworzenia historii pomiarów, alarmów i zdarzeń diagnostycznych.

Odbiór czujników meteorologicznych musi obejmować testy funkcjonalne, techniczne, transmisyjne, diagnostyczne, integracyjne i pomiarowe. W szczególności należy potwierdzić poprawność montażu, poprawność lokalizacji względem przesłon terenowych, poprawność zasilania, działanie funkcji podgrzewania, poprawność komunikacji z systemem RIS, przekazywanie danych pomiarowych, działanie statusów jakości danych, działanie alarmów, możliwość konfiguracji interwałów pomiarowych, poprawność rejestracji danych, poprawność integracji z systemami centralnymi RIS oraz zgodność dokumentacji powykonawczej ze stanem rzeczywistym.

W ramach odbioru Generalny Wykonawca zobowiązany jest przekazać Zamawiającemu co najmniej: protokoły montażu, protokoły konfiguracji, protokoły testów, wykaz nastaw urządzeń, wyniki odczytów testowych, dokumentację powykonawczą lokalizacji, dokumentację tras kablowych, schematy zasilania i transmisji danych, dokumentację konfiguracji, dokumentację integracji z systemem RIS, instrukcje eksploatacyjne, instrukcje diagnostyczne oraz procedury okresowej kontroli i utrzymania sensorów meteorologicznych.

W okresie gwarancji i rękojmi Generalny Wykonawca zobowiązany jest zapewnić okresową kontrolę, konserwację, diagnostykę i weryfikację poprawności pracy czujników

meteorologicznych. Czynności te muszą obejmować co najmniej sprawdzenie stanu mechanicznego czujnika i konstrukcji montażowej, sprawdzenie tras kablowych, sprawdzenie zasilania i podgrzewania, sprawdzenie transmisji danych, sprawdzenie statusów diagnostycznych, kontrolę poprawności raportowania danych oraz aktualizację dokumentacji w przypadku zmian konfiguracji albo wymiany urządzeń.

Szczegółowe rozwiązania projektowe, typy urządzeń, miejsca montażu, sposób prowadzenia tras kablowych, sposób zasilania, sposób transmisji danych, parametry konfiguracji, sposób integracji z systemem RIS oraz procedury odbioru i utrzymania muszą zostać określone przez Generalnego Wykonawcę w dokumentacji projektowej, wykonawczej, powykonawczej, konfiguracyjnej, odbiorowej i eksploatacyjnej oraz zaakceptowane przez Zamawiającego.

1.2.8. Wymagania dla wież, masztów, konstrukcji wsporczych i terenowej infrastruktury teletechnicznej

Rozdział określa wymagania Zamawiającego dotyczące infrastruktury terenowej systemu RIS stanowiącej platformę techniczną dla montażu, zasilania, zabezpieczenia, transmisji danych, eksploatacji i utrzymania urządzeń instalowanych w nowych oraz modernizowanych lokalizacjach systemu RIS. Wymagania te mają charakter przekrojowy i dotyczą w szczególności infrastruktury niezbędnej do funkcjonowania systemów łączności radiowej VHF/AIS/DGNSS, monitoringu wizyjnego CCTV, czujników hydrologicznych, sensorów meteorologicznych, urządzeń transmisji danych, urządzeń zasilania, elementów ochrony odgromowej i przepięciowej, systemów monitoringu technicznego oraz urządzeń pomocniczych.

Infrastruktura objęta niniejszym rozdziałem obejmuje w szczególności obiekty wieżowe stacji radiokomunikacyjnych, maszty, słupy kamerowe, szafy teletechniczne typu zewnętrznego, konstrukcje wsporcze, konstrukcje montażowe, wsporniki, wysięgniki, uchwyty, elementy prowadzenia torów antenowych i kablowych, fundamenty, ogrodzenia, zabezpieczenia techniczne, elementy dostępu serwisowego oraz inne elementy terenowe niezbędne do prawidłowej pracy urządzeń systemu RIS.

Wymagania określone w niniejszym rozdziale należy stosować łącznie z wymaganiami właściwymi dla poszczególnych podsystemów RIS, w szczególności z wymaganiami dotyczącymi systemu łączności radiowej VHF/AIS/DGNSS, systemu monitoringu wizyjnego CCTV, sieci połączeń transmisyjnych, czujników hydrologicznych, sensorów meteorologicznych, zasilania, ochrony odgromowej, uziemienia, ochrony przepięciowej, monitoringu technicznego, dokumentacji, testów, odbiorów, gwarancji, serwisu i utrzymania. Infrastruktura terenowa nie może być projektowana jako zbiór niezależnych elementów montażowych, lecz jako integralna część lokalizacji systemu RIS, powiązana funkcjonalnie, technicznie i eksploatacyjnie z urządzeniami instalowanymi w danej lokalizacji.

Generalny Wykonawca zobowiązany jest zaprojektować i wykonać infrastrukturę terenową w sposób zapewniający jej trwałość, bezpieczeństwo, odporność środowiskową, dostępność serwisową, możliwość prowadzenia przeglądów i konserwacji, ochronę przed dostępem osób nieuprawnionych, poprawność pracy urządzeń oraz zgodność z wymaganiami właścicieli i zarządców nieruchomości, obiektów mostowych, hydrotechnicznych, drogowych, kolejowych albo innych obiektów wykorzystywanych na potrzeby systemu RIS.

Rozwiązania projektowe muszą zostać każdorazowo dostosowane do warunków lokalnych, w szczególności do funkcji lokalizacji w systemie RIS, wymaganej wysokości montażu anten, kamer i sensorów, wyników analiz propagacyjnych i transmisyjnych, wymagań separacji antenowej, wymagań pomiarowych, warunków terenowych, gruntowo-wodnych, hydrologicznych, zalewowych, konstrukcyjnych, środowiskowych, energetycznych, transmisyjnych, formalnoprawnych oraz eksploatacyjnych. Dotyczy to zarówno nowych obiektów i konstrukcji, jak i infrastruktury instalowanej na obiektach istniejących.

Generalny Wykonawca zobowiązany jest uwzględnić, że część lokalizacji systemu RIS będzie zlokalizowana na terenach nadwodnych, hydrotechnicznych, mostowych, zalewowych albo narażonych na okresowe oddziaływanie wody, wilgoci, lodu, wiatru, oblodzenia, drgań i podwyższonej korozyjności środowiska. Dobór konstrukcji, materiałów, zabezpieczeń antykorozyjnych, sposobu posadowienia, wysokości montażu urządzeń, prowadzenia kabli, lokalizacji szaf teletechnicznych oraz sposobu zabezpieczenia terenu musi uwzględniać te uwarunkowania.

Wszystkie elementy infrastruktury terenowej muszą być zaprojektowane i wykonane w sposób zapewniający możliwość bezpiecznego montażu, uruchomienia, eksploatacji, diagnostyki, konserwacji, przeglądów, naprawy i wymiany urządzeń. Dotyczy to w szczególności zapewnienia dostępu serwisowego, bezpiecznej pracy na wysokości, możliwości stosowania systemów asekuracyjnych, właściwego prowadzenia tras kablowych, możliwości wykonywania pomiarów, kontroli stanu technicznego oraz obsługi urządzeń bez konieczności nieuzasadnionej ingerencji w konstrukcję obiektu albo demontażu elementów niezwiązanych z daną czynnością.

Wymagania określone w niniejszym rozdziale obejmują także obowiązek opracowania przez Generalnego Wykonawcę kompletnej dokumentacji projektowej, wykonawczej, powykonawczej, konfiguracyjnej, eksploatacyjnej, odbiorowej i utrzymaniowej dla infrastruktury terenowej. Dokumentacja ta musi jednoznacznie wskazywać przyjęte rozwiązania konstrukcyjne, montażowe, materiałowe, antykorozyjne, zasilające, uziemiające, odgromowe, przepięciowe, kablowe, transmisyjne, zabezpieczające, serwisowe i eksploatacyjne dla każdej lokalizacji.

Przed wykonaniem infrastruktury terenowej Generalny Wykonawca zobowiązany jest przedstawić Zamawiającemu do akceptacji rozwiązania projektowe dotyczące danej lokalizacji, w tym sposób posadowienia albo mocowania, dobór konstrukcji, dobór szafy teletechnicznej, sposób prowadzenia torów antenowych i kablowych, sposób zasilania, uziemienia i ochrony przepięciowej, sposób zabezpieczenia antykorozyjnego, organizację dostępu serwisowego, sposób zabezpieczenia przed dostępem osób nieuprawnionych oraz zakres wymaganych uzgodnień z właścicielem lub zarządcą obiektu.

Akceptacja dokumentacji przez Zamawiającego nie zwalnia Generalnego Wykonawcy z odpowiedzialności za prawidłowość, kompletność, trwałość, bezpieczeństwo, zgodność z przepisami, zgodność z normami, zgodność z warunkami zarządców oraz przydatność infrastruktury terenowej do pracy w systemie RIS. Generalny Wykonawca ponosi odpowiedzialność za zapewnienie, że wykonane wieże, maszty, słupy, szafy, konstrukcje wsporcze, fundamenty, trasy kablowe, zabezpieczenia i pozostałe elementy infrastruktury terenowej będą umożliwiały osiągnięcie wymaganych funkcji i parametrów pracy podsystemów RIS.

Szczegółowe wymagania dotyczące poszczególnych kategorii infrastruktury terenowej określono w kolejnych podrozdziałach niniejszego rozdziału, obejmujących wymagania techniczne dla obiektów wieżowych stacji radiokomunikacyjnych, słupów kamerowych o wysokości 6 m, szaf teletechnicznych typu zewnętrznego oraz konstrukcji wsporczych.

1.2.8.1. Wymagania techniczne dla obiektów wieżowych stacji radiokomunikacyjnych

Generalny Wykonawca zobowiązany jest zaprojektować, uzgodnić, wykonać, dostarczyć, posadowić, wyposażyć, uruchomić, przetestować i przekazać do eksploatacji wolnostojące wieże stalowe ocynkowane ogniowo, przeznaczone do instalacji urządzeń systemu RIS, w szczególności anten VHF, anten AIS, anten DGNSS/GNSS, anten transmisyjnych, sensorów meteorologicznych, kamer, torów antenowych, przewodów sygnałowych, instalacji odgromowej, urządzeń pomocniczych oraz konstrukcji wsporczych wymagających wyniesienia na wysokość.

Wieże muszą zostać zaprojektowane jako kompletne obiekty infrastruktury technicznej, obejmujące co najmniej konstrukcję stalową, fundament, platformę techniczną, drabinę wewnętrzną, system asekuracyjny, system prowadzenia torów antenowych i okablowania, konstrukcje wsporcze dla urządzeń, system ochrony odgromowej i uziemiającej, oznakowanie przeszkodowe, zabezpieczenie antykorozyjne, ogrodzenie terenu, rozwiązania zapewniające bezpieczny dostęp serwisowy oraz dokumentację projektową, wykonawczą, powykonawczą i eksploatacyjną.

Wieże muszą być projektowane indywidualnie dla każdej lokalizacji, z uwzględnieniem funkcji danej lokalizacji w systemie RIS, wymaganej wysokości wyniesienia anten i sensorów, wyników analiz propagacyjnych, wymagań separacji antenowej, warunków gruntowo-wodnych, warunków zalewowych, oddziaływań wiatru i oblodzenia, wymagań zarządców nieruchomości, wymagań formalnoprawnych oraz wymagań eksploatacyjnych Zamawiającego.

1.2.8.1.1. Wysokość i geometria wieży

Główna konstrukcja wieży wolnostojącej musi mieć wysokość wynikającą z dokumentacji projektowej, analiz propagacyjnych, wymagań funkcjonalnych systemów VHF/AIS/DGNSS, wymagań transmisji danych oraz warunków lokalizacyjnych. Minimalna wysokość głównej konstrukcji wieży nie może być mniejsza niż:

1) 30 m – dla lokalizacji, w których analizy projektowe i propagacyjne potwierdzą, że taka wysokość zapewnia spełnienie wymagań systemu RIS;
2) 40 m – dla lokalizacji, w których wymagane jest większe wyniesienie anten, sensorów albo urządzeń transmisyjnych w celu spełnienia wymagań zasięgowych, propagacyjnych, separacyjnych, transmisyjnych lub eksploatacyjnych.

Wysokość całkowita obiektu musi uwzględniać nie tylko wysokość głównej konstrukcji wieży, lecz również platformę techniczną, elementy konstrukcyjne systemu asekuracyjnego, konstrukcje wsporcze urządzeń oraz zwód pionowy instalacji piorunochronnej wyniesiony ponad najwyżej położone elementy antenowe i konstrukcyjne wieży.

Szerokość najwyższego segmentu wieży nie może być mniejsza niż 1,0 m, chyba że Generalny Wykonawca wykaże w dokumentacji projektowej, że inne rozwiązanie zapewnia co najmniej równoważną nośność, stateczność, bezpieczeństwo obsługi, możliwość montażu urządzeń, zachowanie wymaganych odległości separacyjnych oraz dostęp serwisowy.

Konstrukcja wieży musi umożliwiać montaż urządzeń na wysokościach wymaganych dla poprawnej pracy poszczególnych podsystemów RIS, w tym dla systemów VHF, AIS, DGNSS/GNSS, transmisji danych, sensorów meteorologicznych oraz kamer, przy zachowaniu wymagań producentów urządzeń, wymagań ochrony odgromowej, wymagań separacji antenowej oraz wymagań bezpieczeństwa pracy na wysokości.

1.2.8.1.2. Konstrukcja stalowa i zabezpieczenie antykorozyjne

Wieża musi być wykonana jako konstrukcja stalowa wolnostojąca, zaprojektowana zgodnie z właściwymi przepisami, normami konstrukcyjnymi, wymaganiami dotyczącymi konstrukcji stalowych oraz zasadami wiedzy technicznej. Konstrukcja musi być dostosowana do pracy całorocznej w warunkach zewnętrznych, w tym w warunkach występowania wiatru, opadów, oblodzenia, zmian temperatury, wilgoci, korozji atmosferycznej oraz oddziaływań środowiskowych typowych dla lokalizacji nadwodnych i terenów zalewowych.

Wszystkie zasadnicze elementy stalowe wieży, platformy technicznej, drabiny, balustrad, wsporników, uchwytów, konstrukcji antenowych, elementów prowadzenia kabli, elementów mocujących oraz wyposażenia konstrukcyjnego muszą być zabezpieczone antykorozyjnie przez cynkowanie ogniowe albo przez rozwiązanie równoważne, zapewniające trwałość i odporność środowiskową nie gorszą niż cynkowanie ogniowe.

Ochrona antykorozyjna musi zostać dobrana do klasy korozyjności środowiska danej lokalizacji, przewidywanego okresu eksploatacji, warunków zalewowych, oddziaływania wilgoci, mgły, zanieczyszczeń atmosferycznych, promieniowania UV oraz czynników związanych z eksploatacją infrastruktury nadwodnej. Generalny Wykonawca zobowiązany jest wskazać w dokumentacji projektowej przyjętą klasę korozyjności, system ochrony antykorozyjnej, technologię wykonania zabezpieczenia oraz zasady kontroli i utrzymania powłok.

Wszystkie połączenia śrubowe, kotwy, pręty gwintowane, elementy mocujące, obejmy i uchwyty muszą być dobrane do obciążeń konstrukcyjnych, zmęczeniowych, montażowych i eksploatacyjnych oraz zabezpieczone przed korozją. Elementy złączne muszą być zgodne z dokumentacją projektową, wymaganiami właściwych norm oraz warunkami pracy konstrukcji.

1.2.8.1.3. Fundament i warunki posadowienia

Wieże muszą być posadowione na fundamentach wylewanych, wykonanych na podstawie dokumentacji projektowej opracowanej przez Generalnego Wykonawcę. Nie dopuszcza się przyjęcia typowego fundamentu bez uprzedniej weryfikacji warunków gruntowo-wodnych, warunków zalewowych, poziomu wód gruntowych, nośności podłoża, głębokości przemarzania, warunków geotechnicznych oraz oddziaływań wynikających z wysokości i wyposażenia wieży.

Parametry fundamentu muszą zostać dobrane indywidualnie dla każdej lokalizacji, z uwzględnieniem co najmniej:

1) wysokości i geometrii wieży;
2) masy konstrukcji stalowej;
3) masy i rozmieszczenia urządzeń montowanych na wieży;
4) obciążeń wiatrem;
5) obciążeń oblodzeniem;
6) obciążeń od platformy technicznej i osób wykonujących czynności serwisowe;
7) oddziaływań dynamicznych i zmęczeniowych;
8) wyników badań geotechnicznych;
9) warunków wodnych i zalewowych;
10) wymagań zarządcy nieruchomości;
11) wymagań trwałości i bezpieczeństwa eksploatacji.

Generalny Wykonawca zobowiązany jest wykonać badania gruntowo-wodne oraz określić geotechniczne warunki posadowienia dla każdej lokalizacji wieży. Zakres badań musi być adekwatny do rodzaju obiektu, wysokości wieży, warunków terenowych, stopnia skomplikowania warunków gruntowych oraz wymagań właściwych przepisów i norm. Wyniki badań muszą zostać uwzględnione w projekcie fundamentu.

Fundament musi być zaprojektowany w sposób odporny na oddziaływania właściwe dla terenów zalewowych, w tym na okresowe podniesienie poziomu wód, zawilgocenie, erozję, podmywanie, wypór, oddziaływanie lodu, utratę nośności gruntu oraz ograniczenia eksploatacyjne wynikające z lokalizacji w sąsiedztwie rzeki albo obiektu hydrotechnicznego.

Wymiary fundamentu oraz zagospodarowanie bezpośredniego otoczenia wieży muszą uwzględniać miejsce na posadowienie szafy teletechnicznej typu zewnętrznego oraz wykonanie kanałów kablowych, przepustów, rur osłonowych albo innych tras kablowych łączących szafę z wieżą, systemami prowadzenia torów antenowych, przewodami zasilającymi, przewodami sygnałowymi, przewodami uziemiającymi oraz instalacją odgromową.

1.2.8.1.4. Platforma techniczna

Każda wieża musi być wyposażona w platformę techniczną umożliwiającą bezpieczny montaż, obsługę, kontrolę, konserwację i wymianę urządzeń instalowanych na wysokości. Platforma musi być zintegrowana z konstrukcją wieży i zaprojektowana z uwzględnieniem obciążeń stałych, użytkowych, serwisowych, wiatrowych, oblodzeniowych, montażowych oraz obciążeń od urządzeń.

Minimalne wymiary rzutu platformy technicznej nie mogą być mniejsze niż 1 500 × 1 500 mm. W przypadku konieczności instalacji większej liczby urządzeń, zapewnienia wymaganych odległości separacyjnych, zapewnienia bezpiecznego dostępu serwisowego albo spełnienia

wymagań producentów urządzeń Generalny Wykonawca zobowiązany jest zastosować platformę o większych wymiarach.

Platforma musi być wyposażona co najmniej w:

1) stabilną konstrukcję nośną;
2) antypoślizgową, ażurową podłogę odporną na zaleganie wody, śniegu i lodu;
3) balustrady ochronne;
4) bortnicę albo cokół zabezpieczający przed zsunięciem narzędzi i elementów montażowych;
5) klapę wejściową albo inny bezpieczny sposób wejścia z drabiny na platformę;
6) uchwyty, wsporniki i konstrukcje montażowe dla anten, sensorów i urządzeń;
7) punkty mocowania środków ochrony indywidualnej, jeżeli wynikają z projektu systemu asekuracyjnego;
8) powiązanie z instalacją odgromową, uziemiającą i połączeniami wyrównawczymi;
9) rozwiązania umożliwiające uporządkowane prowadzenie torów antenowych i okablowania.

Platforma musi zapewniać możliwość bezpiecznego wykonywania czynności serwisowych przez osoby posiadające wymagane kwalifikacje do pracy na wysokości. Rozwiązanie nie może wymagać demontażu podstawowych elementów konstrukcji wieży w celu uzyskania dostępu do urządzeń.

1.2.8.1.5. Drabina wewnętrzna i komunikacja pionowa

Wieża musi być wyposażona w wewnętrzną drabinę umożliwiającą poruszanie się po konstrukcji wieży i dostęp do platformy technicznej. Drabina musi być zaprojektowana jako element stały, trwale połączony z konstrukcją wieży, odporny na korozję, obciążenia użytkowe, wpływ warunków atmosferycznych oraz pracę w warunkach zewnętrznych.

Drabina musi zapewniać bezpieczne wejście i zejście z wieży oraz współpracować z systemem asekuracyjnym. Lokalizacja, szerokość, rozstaw szczebli, sposób mocowania, odległości od konstrukcji oraz strefy przejścia muszą spełniać wymagania przepisów BHP, właściwych norm oraz dokumentacji projektowej.

Wejście na drabinę musi być zabezpieczone przed dostępem osób nieuprawnionych. Sposób zabezpieczenia musi być uzgodniony z Zamawiającym i dostosowany do organizacji ochrony danej lokalizacji.

1.2.8.1.6. System asekuracyjny

Wieża musi być wyposażona w stały system asekuracyjny umożliwiający bezpieczne wejście, zejście i wykonywanie czynności serwisowych przez osoby uprawnione do pracy na wysokości.

System asekuracyjny musi być zgodny z obowiązującymi przepisami, wymaganiami BHP, wymaganiami producenta systemu oraz właściwymi normami dotyczącymi ochrony przed upadkiem z wysokości.

W wieżach antenowych eksploatowanych na obszarze Dolnej Odry stosowane jest rozwiązanie typu pionowego systemu asekuracji linowej 3M™ Protecta® Cabloc Cable Vertical Safety System. Informacja ta ma charakter opisu stanu istniejącego oraz punktu odniesienia dla zachowania kompatybilności eksploatacyjnej, organizacji serwisu, wyposażenia pracowników i sposobu utrzymania. Nie oznacza ona obowiązku zastosowania konkretnego produktu, o ile Generalny Wykonawca zapewni system równoważny funkcjonalnie, technicznie, użytkowo i eksploatacyjnie, zaakceptowany przez Zamawiającego.

System asekuracyjny musi obejmować co najmniej:

1) prowadnicę pionową albo równoważny element systemu asekuracji;
2) linę, szynę albo inny element prowadzący zgodny z przyjętym systemem;
3) absorber energii albo równoważny element ograniczający skutki upadku;
4) elementy mocujące do konstrukcji wieży;
5) kompletne oznakowanie systemu;
6) instrukcję użytkowania i konserwacji;
7) dokumentację zgodności;
8) protokoły montażu, kontroli i odbioru;
9) zasady okresowych przeglądów i dopuszczania systemu do użytkowania.

System asekuracyjny musi być objęty dokumentacją eksploatacyjną oraz planem przeglądów i aktualizacji. Generalny Wykonawca zobowiązany jest przekazać Zamawiającemu instrukcje użytkowania, zasady kontroli przed użyciem, wymagania dotyczące środków ochrony indywidualnej kompatybilnych z systemem oraz wymagania dotyczące przeglądów okresowych.

1.2.8.1.7. System prowadzenia torów antenowych i okablowania

Wieża musi być wyposażona w system prowadzenia torów antenowych, kabli koncentrycznych, światłowodów, przewodów sygnałowych, przewodów zasilających, przewodów sterujących, przewodów uziemiających oraz innych przewodów wymaganych dla urządzeń montowanych na wieży.

System prowadzenia torów antenowych i okablowania musi być dobrany do specyfiki poszczególnych urządzeń, w szczególności anten VHF, anten AIS, anten DGNSS/GNSS, anten transmisyjnych, sensorów meteorologicznych, kamer, elementów monitoringu technicznego oraz urządzeń pomocniczych.

Trasy kablowe muszą być prowadzone w sposób uporządkowany, trwały, identyfikowalny, odporny na uszkodzenia mechaniczne, promieniowanie UV, wilgoć, oblodzenie, zmiany temperatury, drgania, naprężenia oraz oddziaływanie wiatru. Trasy kablowe nie mogą utrudniać

korzystania z drabiny, systemu asekuracyjnego, platformy technicznej ani dostępu serwisowego do urządzeń.

System prowadzenia kabli musi obejmować co najmniej:

1) koryta, drabinki, uchwyty, obejmy, prowadnice albo inne elementy prowadzenia kabli;
2) ochronę kabli na przejściach przez fundament, szafę, konstrukcję wieży i platformę;
3) punkty mocowania zapewniające brak niekontrolowanego przemieszczania kabli;
4) zachowanie wymaganych promieni gięcia;
5) separację kabli zasilających, sygnałowych, antenowych i uziemiających, jeżeli jest wymagana;
6) oznakowanie kabli i torów;
7) możliwość kontroli i wymiany kabli bez ingerencji w zasadniczą konstrukcję wieży;
8) zabezpieczenie przejść kablowych przed wnikaniem wody, zanieczyszczeń, owadów i gryzoni.

1.2.8.1.8. Konstrukcje wsporcze dla anten, sensorów i urządzeń

Wieża musi być wyposażona w konstrukcje wsporcze umożliwiające montaż wszystkich urządzeń przewidzianych dla danej lokalizacji. Konstrukcje wsporcze muszą być zaprojektowane indywidualnie dla urządzeń instalowanych na wieży, z uwzględnieniem ich masy, powierzchni czynnej, obciążeń wiatrem, wymagań separacji, wymagań producentów, dostępu serwisowego oraz wymagań ochrony odgromowej.

Konstrukcje wsporcze muszą umożliwiać montaż co najmniej:

1) anten VHF;
2) anten AIS;
3) anten DGNSS/GNSS;
4) anten transmisyjnych;
5) sensorów meteorologicznych;
6) kamer, jeżeli dana lokalizacja pełni funkcję obserwacyjną lub dozorową;
7) torów antenowych i kablowych;
8) elementów instalacji odgromowej;
9) urządzeń pomocniczych wynikających z dokumentacji projektowej.

Rozmieszczenie urządzeń na wieży musi zapewniać spełnienie wymagań propagacyjnych, separacyjnych, elektromagnetycznych, eksploatacyjnych i serwisowych. Nie dopuszcza się takiego zagęszczenia urządzeń, które uniemożliwiałoby bezpieczny dostęp serwisowy, powodowałoby wzajemne zakłócenia, utrudniało prowadzenie kabli albo ograniczało skuteczność ochrony odgromowej.

1.2.8.1.9. Ochrona odgromowa, uziemienie i połączenia wyrównawcze

Wieża musi być wyposażona w system ochrony odgromowej o wysokim prawdopodobieństwie ochrony przed skutkami bezpośredniego wyładowania atmosferycznego. System ochrony odgromowej musi obejmować zwód pionowy wyniesiony ponad najwyżej położone elementy antenowe i konstrukcyjne wieży, przewody odprowadzające, uziom, połączenia wyrównawcze, ochronę przepięciową oraz połączenia ochronne urządzeń elektronicznych.

Projekt ochrony odgromowej musi zostać opracowany na podstawie analizy ryzyka oraz właściwych norm i przepisów. Klasa ochrony odgromowej, geometria zwodów, sposób prowadzenia przewodów odprowadzających, liczba punktów uziemienia, parametry uziomu oraz dobór ochronników przepięciowych muszą wynikać z dokumentacji projektowej.

Wieża musi być wyposażona w zaciski do rozłącznego dołączania punktów uziomowych montowanych urządzeń elektronicznych, anten, szaf, konstrukcji wsporczych, ekranów kablowych, torów antenowych i innych elementów wymagających uziemienia albo połączeń wyrównawczych. Zaciski muszą być dostępne do kontroli, oznakowane, odporne na korozję oraz dostosowane do przewidywanych przekrojów przewodów.

Instalacja uziemiająca musi być skoordynowana z fundamentem, szafą teletechniczną, trasami kablowymi, instalacją zasilającą, torami antenowymi, systemem ochrony przepięciowej oraz wymaganiami producentów urządzeń. Dokumentacja powykonawcza musi zawierać wyniki pomiarów rezystancji uziemienia oraz protokoły sprawdzeń ochrony odgromowej i przeciwprzepięciowej.

1.2.8.1.10. Oznakowanie przeszkodowe i malowanie przeszkodowe

Każda wieża musi zostać zweryfikowana pod kątem wymagań dotyczących przeszkód lotniczych, oznakowania przeszkodowego i ewentualnego malowania przeszkodowego. Generalny Wykonawca zobowiązany jest ustalić, czy dla danej lokalizacji, wysokości obiektu, uwarunkowań lotniczych, korytarzy lotniczych, sąsiedztwa lotnisk, lądowisk, heliportów albo innych stref wymagane jest oznakowanie dzienne, oznakowanie świetlne, malowanie przeszkodowe lub inne środki wymagane przez właściwe organy.

Wieża musi być wyposażona w oznakowanie przeszkodowe, jeżeli jest ono wymagane przepisami, decyzjami, uzgodnieniami albo warunkami właściwego organu. Oznakowanie przeszkodowe musi zostać ujęte w dokumentacji projektowej, zasilaniu, monitoringu technicznym, dokumentacji eksploatacyjnej oraz procedurach utrzymania.

Malowanie przeszkodowe należy wykonać wyłącznie wtedy, gdy jest ono wymagane dla danej lokalizacji albo wynika z decyzji, uzgodnień, warunków technicznych lub przepisów. Jeżeli malowanie przeszkodowe jest wymagane, musi być kompatybilne z systemem ochrony antykorozyjnej i nie może obniżać trwałości cynkowania ogniowego albo innych zabezpieczeń antykorozyjnych.

1.2.8.1.11. Ogrodzenie i zabezpieczenie terenu

Teren posadowienia wieży oraz dodatkowa przestrzeń ją otaczająca, uzgodniona z właścicielem albo zarządcą lokalizacji, musi zostać wygrodzona ogrodzeniem o wysokości nie mniejszej niż 2,2 m. W uzasadnionych przypadkach, wynikających z wymagań bezpieczeństwa, lokalizacji, ryzyka dostępu osób nieuprawnionych albo warunków zarządcy, ogrodzenie powinno mieć wysokość do 3,0 m.

Ogrodzenie musi być wyposażone w furtkę umożliwiającą wejście na teren wieży. Furtka musi być zamykana na klucz patentowy albo inny system kontroli dostępu zaakceptowany przez Zamawiającego. System zamknięcia musi być spójny z zasadami zarządzania dostępem do infrastruktury RIS.

W lokalizacjach wymagających szczególnej ochrony ogrodzenie musi być zakończone drutem kolczastym albo innym równoważnym zabezpieczeniem na konstrukcji wsporczej w kształcie litery Y, o ile rozwiązanie takie jest dopuszczalne przez przepisy, warunki zarządcy nieruchomości i uzgodnienia lokalizacyjne.

Ogrodzenie musi zostać zaprojektowane w sposób odporny na warunki zewnętrzne, korozję, uszkodzenia mechaniczne, próby nieuprawnionego wejścia, okresowe zawilgocenie oraz oddziaływania środowiskowe właściwe dla lokalizacji nadwodnych i zalewowych. Posadowienie ogrodzenia musi uwzględniać warunki gruntowo-wodne oraz możliwość okresowego zalania terenu.

1.2.8.1.12. Szafa teletechniczna i powiązanie z wieżą

Projekt lokalizacji wieży musi uwzględniać posadowienie szafy teletechnicznej typu zewnętrznego, przeznaczonej do instalacji urządzeń radiowych, transmisyjnych, zasilających, zabezpieczających, monitorujących i sterujących, jeżeli takie urządzenia są przewidziane dla danej lokalizacji.

Szafa teletechniczna musi być usytuowana w sposób umożliwiający bezpieczne prowadzenie kabli pomiędzy szafą i wieżą, dostęp serwisowy, ochronę przed uszkodzeniami mechanicznymi, ochronę przed zalaniem w zakresie wynikającym z warunków lokalizacyjnych oraz zachowanie wymagań producentów urządzeń.

Kanały kablowe, przepusty, rury osłonowe i inne elementy prowadzenia przewodów pomiędzy szafą a wieżą muszą być zaprojektowane i wykonane jako element integralny lokalizacji. Muszą one zapewniać ochronę kabli przed uszkodzeniem, wodą, wilgocią, promieniowaniem UV, gryzoniami, naprężeniami, oblodzeniem oraz przypadkową ingerencją osób trzecich.

1.2.8.1.13. Tablice informacyjne i oznakowanie projektu

Wszystkie lokalizacje wież muszą być wyposażone w tablice informacyjne zawierające wymagane dane projektowe oraz informację o współfinansowaniu ze środków Unii Europejskiej. Tablice muszą być zgodne z aktualnymi wytycznymi dotyczącymi oznakowania projektów

współfinansowanych ze środków UE, wymaganiami Zamawiającego oraz dokumentacją projektową.

Tablice muszą być wykonane z materiałów odpornych na warunki zewnętrzne, promieniowanie UV, wilgoć, korozję, zmiany temperatury i uszkodzenia mechaniczne. Muszą być zamontowane w miejscu widocznym, trwałym i bezpiecznym, uzgodnionym z Zamawiającym oraz właścicielem albo zarządcą lokalizacji.

Oprócz tablic informacyjnych należy przewidzieć oznakowanie eksploatacyjne i ostrzegawcze, obejmujące co najmniej informacje o zakazie wstępu osobom nieupoważnionym, pracy urządzeń radiowych, zagrożeniu porażeniowym, pracy na wysokości, konieczności stosowania środków ochrony indywidualnej oraz dane kontaktowe służb utrzymaniowych, jeżeli Zamawiający wymaga takiego oznakowania.

1.2.8.1.14. Wymagania formalne i projektowe

Generalny Wykonawca zobowiązany jest opracować kompletną dokumentację projektową dla każdej wieży, obejmującą co najmniej:

1) projekt zagospodarowania terenu;
2) projekt architektoniczno-budowlany, jeżeli jest wymagany;
3) projekt techniczny;
4) projekt wykonawczy;
5) obliczenia konstrukcyjne wieży, platformy i fundamentu;
6) dokumentację geotechniczną;
7) projekt ochrony odgromowej i uziemienia;
8) projekt tras kablowych i torów antenowych;
9) projekt szafy teletechnicznej i powiązań kablowych;
10) projekt ogrodzenia;
11) projekt oznakowania przeszkodowego, jeżeli jest wymagany;
12) projekt organizacji dostępu serwisowego i systemu asekuracyjnego;
13) zestawienie urządzeń montowanych na wieży;
14) zestawienie obciążeń od urządzeń;
15) opis zabezpieczeń antykorozyjnych;
16) wymagane uzgodnienia, zgody, opinie i decyzje administracyjne.

Generalny Wykonawca zobowiązany jest uzyskać wszystkie wymagane zgody, uzgodnienia, decyzje, pozwolenia, warunki techniczne, opinie, odstępstwa i zatwierdzenia niezbędne do zaprojektowania, budowy, wyposażenia, uruchomienia i przekazania wieży do eksploatacji.

1.2.8.1.15. Wymagania odbiorowe

Odbiór wieży musi obejmować co najmniej:

1) weryfikację zgodności lokalizacji z dokumentacją projektową;
2) weryfikację fundamentu i jego powiązania z dokumentacją geotechniczną;
3) weryfikację konstrukcji stalowej;
4) weryfikację zabezpieczenia antykorozyjnego;
5) weryfikację wysokości wieży;
6) weryfikację szerokości najwyższego segmentu;
7) weryfikację platformy technicznej;
8) weryfikację drabiny i systemu asekuracyjnego;
9) weryfikację konstrukcji wsporczych anten i sensorów;
10) weryfikację systemu prowadzenia torów antenowych i okablowania;
11) weryfikację instalacji odgromowej, uziemiającej i połączeń wyrównawczych;
12) wykonanie pomiarów elektrycznych i uziemiających;
13) weryfikację oznakowania przeszkodowego, jeżeli jest wymagane;
14) weryfikację ogrodzenia i zabezpieczenia terenu;
15) weryfikację tablic informacyjnych i oznakowania projektu;
16) weryfikację dokumentacji powykonawczej;
17) przekazanie instrukcji eksploatacji, instrukcji BHP i procedur serwisowych;
18) przekazanie dokumentów gwarancyjnych, certyfikatów, deklaracji zgodności i protokołów kontroli.

Odbiór wieży może nastąpić wyłącznie po potwierdzeniu, że obiekt jest kompletny, bezpieczny, zgodny z dokumentacją projektową, przygotowany do montażu i eksploatacji urządzeń systemu RIS oraz dopuszczony do użytkowania w zakresie wymaganym przez przepisy prawa i decyzje właściwych organów.

1.2.8.1.16. Przeglądy techniczne, kontrole okresowe i utrzymanie wież w okresie realizacji oraz gwarancji

Generalny Wykonawca zobowiązany jest w okresie realizacji przedmiotu zamówienia oraz w całym okresie świadczenia gwarancji wykonywać, na własny koszt i ryzyko, wszelkie przeglądy techniczne, kontrole okresowe, czynności utrzymaniowe, konserwacyjne, pomiarowe i serwisowe wymagane dla wolnostojących wież stalowych, ich fundamentów, wyposażenia technicznego, instalacji, systemów bezpieczeństwa oraz elementów zamontowanych na konstrukcji wieży.

Obowiązek ten obejmuje w szczególności przeglądy i kontrole wymagane przepisami prawa, warunkami decyzji administracyjnych, dokumentacją projektową, dokumentacją techniczno-ruchową, instrukcjami producentów, dokumentacją eksploatacyjną, zasadami wiedzy technicznej oraz wymaganiami właściwych norm i standardów mających zastosowanie do tego typu konstrukcji i wyposażenia.

Zakres przeglądów, kontroli i czynności utrzymaniowych musi obejmować co najmniej:

1) kontrolę stanu technicznego konstrukcji stalowej wieży;
2) kontrolę stanu fundamentu, zakotwień, połączeń śrubowych, elementów mocujących i elementów konstrukcyjnych;
3) kontrolę stanu zabezpieczeń antykorozyjnych, w tym powłok cynkowych i ewentualnych powłok malarskich;
4) kontrolę platformy technicznej, balustrad, bortnic, klap, pomostów, podłóg ażurowych, uchwytów i elementów wsporczych;
5) kontrolę drabiny wewnętrznej, przejść, punktów dostępu oraz elementów komunikacji pionowej;
6) kontrolę, konserwację i okresowe dopuszczenie do użytkowania systemu asekuracyjnego oraz elementów ochrony przed upadkiem z wysokości;
7) kontrolę konstrukcji wsporczych anten, sensorów, kamer, urządzeń transmisyjnych i pozostałych urządzeń montowanych na wieży;
8) kontrolę systemu prowadzenia torów antenowych, kabli, przewodów sygnałowych, przewodów zasilających, światłowodów, uchwytów, obejm i przepustów;
9) kontrolę instalacji odgromowej, uziemiającej, połączeń wyrównawczych, zacisków rozłącznych oraz ochrony przepięciowej;
10) wykonanie wymaganych pomiarów elektrycznych, pomiarów rezystancji uziemienia, pomiarów ciągłości połączeń ochronnych oraz innych pomiarów wymaganych dla danego typu instalacji;
11) kontrolę oznakowania przeszkodowego, oświetlenia przeszkodowego, malowania przeszkodowego oraz tablic informacyjnych i ostrzegawczych, jeżeli występują;
12) kontrolę ogrodzenia, furtki, zamknięć, zabezpieczeń przed dostępem osób nieuprawnionych oraz oznakowania terenu;
13) kontrolę szafy teletechnicznej, kanałów kablowych, przepustów, rur osłonowych i powiązań kablowych pomiędzy szafą a wieżą, w zakresie dotyczącym bezpieczeństwa i integralności infrastruktury wieżowej;
14) usunięcie stwierdzonych usterek, uszkodzeń, luzów, korozji, odkształceń, braków oznakowania, braków zabezpieczeń oraz innych nieprawidłowości mogących wpływać na bezpieczeństwo, trwałość, dostępność albo prawidłową eksploatację wieży i jej wyposażenia.

Generalny Wykonawca zobowiązany jest opracować i przekazać Zamawiającemu harmonogram przeglądów i kontroli okresowych dla każdej wieży, uwzględniający wymagania przepisów prawa,

dokumentacji producentów, dokumentacji projektowej, dokumentacji eksploatacyjnej, systemu asekuracyjnego, instalacji odgromowej, instalacji uziemiającej, oznakowania przeszkodowego oraz pozostałego wyposażenia technicznego. Harmonogram ten musi zostać ujęty w Szczegółowym Planie Przeglądów i Aktualizacji oraz w Dokumentacji Eksploatacyjnej systemu RIS.

Każdy przegląd, kontrola, pomiar, czynność konserwacyjna i czynność serwisowa musi zostać udokumentowana protokołem. Protokół musi zawierać co najmniej datę wykonania czynności, lokalizację, zakres wykonanych prac, dane osób wykonujących przegląd, podstawę wykonania przeglądu, opis stanu technicznego, wykaz stwierdzonych nieprawidłowości, zalecenia, termin usunięcia nieprawidłowości, wyniki pomiarów, dokumentację fotograficzną oraz potwierdzenie usunięcia usterek, jeżeli zostały stwierdzone.

Przeglądy i kontrole wymagające udziału osób posiadających szczególne kwalifikacje, uprawnienia budowlane, uprawnienia elektryczne, uprawnienia do kontroli systemów asekuracyjnych, uprawnienia do pracy na wysokości albo inne kwalifikacje wymagane przepisami prawa lub dokumentacją producenta muszą być wykonywane wyłącznie przez osoby posiadające wymagane kwalifikacje i uprawnienia.

Wykonanie przeglądów, kontroli, pomiarów i czynności utrzymaniowych nie zwalnia Generalnego Wykonawcy z odpowiedzialności gwarancyjnej za wieże, ich fundamenty, konstrukcje, wyposażenie, instalacje oraz urządzenia zamontowane na wieżach. Brak wykonania wymaganego przeglądu, kontroli, pomiaru albo czynności utrzymaniowej w wymaganym terminie stanowi nienależyte wykonanie obowiązków Generalnego Wykonawcy.

Generalny Wykonawca zobowiązany jest przekazywać Zamawiającemu protokoły z przeglądów, kontroli i pomiarów niezwłocznie po ich wykonaniu, nie później jednak niż w terminie określonym w umowie albo zaakceptowanym harmonogramie utrzymania. Dokumentacja z przeglądów i kontroli stanowi część dokumentacji eksploatacyjnej systemu RIS i musi być aktualizowana przez cały okres gwarancji.

1.2.8.2. Wymagania techniczne dla słupa kamerowego o wysokości 6 m

Słup kamerowy musi być przeznaczony do montażu kamer systemu monitoringu wizyjnego CCTV w warunkach zewnętrznych. Konstrukcja słupa musi umożliwiać instalację co najmniej kilku kamer CCTV na belce poprzecznej, wysięgniku, obejmach montażowych albo innym systemowym elemencie montażowym dostosowanym do rodzaju zastosowanych kamer.

Słup musi mieć wysokość nominalną 6 m, liczoną od poziomu posadowienia do poziomu górnej części konstrukcji nośnej. Wysokość ta musi umożliwiać uzyskanie wymaganego pola widzenia kamer, ograniczenie ryzyka zasłaniania obrazu przez osoby, pojazdy, elementy małej architektury lub roślinność oraz zapewnienie stabilnej obserwacji wskazanego obszaru.

Konstrukcja słupa musi być wykonana jako konstrukcja samonośna, wolnostojąca, przystosowana do pracy w warunkach zewnętrznych. Dopuszcza się zastosowanie konstrukcji kratownicowej zbieżnej, aluminiowej albo równoważnej konstrukcji metalowej o parametrach nośności, sztywności, odporności korozyjnej i trwałości nie gorszych niż wymagane dla lokalizacji objętej projektem.

Słup musi zapewniać odpowiednią sztywność i stabilność pracy kamer. Konstrukcja nie może powodować drgań, wychyleń ani odkształceń, które wpływają na pogorszenie jakości obrazu, stabilność kadru, działanie funkcji analitycznych, skuteczność kompresji wideo albo możliwość prowadzenia obserwacji w warunkach wiatrowych typowych dla lokalizacji montażu.

Słup musi być wykonany z materiału odpornego na korozję i oddziaływanie warunków atmosferycznych. W przypadku zastosowania aluminium materiał konstrukcyjny musi odpowiadać co najmniej klasie AW6082 albo równoważnej pod względem wytrzymałości i odporności środowiskowej. Elementy stalowe, złączne, kotwiące i montażowe muszą być zabezpieczone antykorozyjnie w sposób właściwy dla zastosowań zewnętrznych.

Minimalne parametry konstrukcyjne słupa muszą odpowiadać następującym wymaganiom:

1) wysokość słupa: 6 m;
2) konstrukcja przeznaczona do montażu kamer CCTV;
3) możliwość montażu kamer na poprzecznej belce instalacyjnej, obejmach cybantowych, wysięgnikach albo rozwiązaniu równoważnym;
4) konstrukcja zbieżna albo równoważna pod względem sztywności;
5) szerokość konstrukcji u podstawy nie mniejsza niż 500 mm dla konstrukcji kratownicowej albo równoważna nośność i sztywność dla innego typu konstrukcji;
6) szerokość konstrukcji w górnej części nie mniejsza niż 250 mm dla konstrukcji kratownicowej albo równoważna nośność i sztywność dla innego typu konstrukcji;
7) masa i geometria konstrukcji dostosowane do bezpiecznego transportu, montażu i eksploatacji;
8) konstrukcja przystosowana do pracy w warunkach zewnętrznych.

Słup musi umożliwiać prowadzenie okablowania kamer w sposób uporządkowany i zabezpieczony. Konstrukcja musi posiadać przepust kablowy, kanał kablowy, krawężnik konstrukcyjny, rury osłonowe albo inne rozwiązanie systemowe umożliwiające sprowadzenie przewodów z kamer do podstawy słupa lub do punktu dystrybucyjnego. Przewody nie mogą być prowadzone luzem po konstrukcji bez ochrony mechanicznej i środowiskowej.

Słup musi umożliwiać doprowadzenie i prowadzenie przewodów zasilających, sygnałowych, teleinformatycznych, uziemiających oraz przewodów ochrony przepięciowej zgodnie z projektem wykonawczym. Wejścia i wyjścia kablowe muszą być zabezpieczone przed wnikaniem wody, śniegu, lodu, owadów, pyłu i innych zanieczyszczeń. Nie dopuszcza się pozostawiania otwartych, niezaślepionych albo nieuszczelnionych zakończeń przepustów kablowych.

Słup musi być przystosowany do posadowienia na fundamencie zapewniającym przeniesienie obciążeń od masy własnej słupa, zamontowanych kamer, wysięgników, osprzętu, parcia wiatru, obciążeń eksploatacyjnych oraz lokalnych warunków gruntowo-wodnych. Fundament musi zostać zaprojektowany przez Generalnego Wykonawcę na podstawie rzeczywistych warunków lokalizacji i wymagań producenta zastosowanego słupa.

Fundament słupa musi zostać wykonany jako fundament żelbetowy, prefabrykowany, monolityczny, fundament na kotwach chemicznych albo inne rozwiązanie równoważne, jeżeli zapewnia wymaganą nośność, stateczność i trwałość. Dobór fundamentu musi uwzględniać lokalne warunki gruntowe, poziom wód gruntowych, ryzyko podmywania, przemarzania, oddziaływania wiatru oraz wymagania właściciela lub zarządcy terenu.

Połączenie słupa z fundamentem musi być wykonane z zastosowaniem kołnierza, płyty podstawy, kotew, śrub, szpilek montażowych albo innego rozwiązania systemowego przewidzianego przez producenta. Połączenie musi umożliwiać bezpieczne przeniesienie obciążeń, trwałe zamocowanie słupa, wypoziomowanie konstrukcji oraz dostęp serwisowy do elementów kotwiących. Elementy kotwiące muszą być zabezpieczone przed korozją.

Słup musi umożliwiać bezpieczny montaż i serwis kamer. Sposób dostępu serwisowego musi zostać określony w dokumentacji projektowej i instrukcji eksploatacji. Jeżeli konstrukcja dopuszcza wejście technika na słup, dostęp ten może odbywać się wyłącznie zgodnie z instrukcją producenta, przepisami BHP, wymaganiami pracy na wysokości oraz przy warunkach atmosferycznych dopuszczonych przez producenta. Dopuszcza się również obsługę serwisową z użyciem podnośnika, drabiny, platformy roboczej albo innego bezpiecznego rozwiązania.

Słup musi umożliwiać montaż osprzętu dodatkowego wymaganego dla punktu kamerowego, w szczególności uchwytów kamer, wysięgników, puszek instalacyjnych, ochronników przepięciowych, obudów połączeniowych, anten pomocniczych, elementów uziemienia, tabliczki identyfikacyjnej oraz zabezpieczeń przed przysiadaniem ptactwa. Osprzęt musi być dobrany w sposób niepowodujący przekroczenia dopuszczalnych obciążeń słupa.

Słup oraz osprzęt montażowy muszą umożliwiać zastosowanie zabezpieczeń ograniczających przysiadanie ptactwa na kamerach, wysięgnikach, belkach montażowych i górnych elementach konstrukcji. Zabezpieczenia te nie mogą ograniczać pola widzenia kamer, nie mogą utrudniać serwisu i nie mogą powodować zagrożenia dla użytkowników ani osób trzecich.

Słup musi być przygotowany do wykonania uziemienia i połączeń wyrównawczych zgodnie z projektem instalacji elektrycznej, wymaganiami ochrony przeciwporażeniowej, ochrony przepięciowej oraz wymaganiami producenta urządzeń. Konstrukcja musi umożliwiać podłączenie przewodu uziemiającego do wskazanego punktu konstrukcji albo instalacji uziemiającej.

Słup musi zostać dostarczony jako wyrób kompletny, obejmujący wszystkie elementy niezbędne do montażu i eksploatacji w danej lokalizacji, w szczególności konstrukcję słupa, elementy połączeniowe, kołnierz lub płytę podstawy, komplet elementów montażowych przewidzianych przez producenta, dokumentację techniczną, instrukcję montażu, instrukcję eksploatacji, kartę katalogową oraz dokumenty potwierdzające parametry techniczne.

Wykończenie powierzchni słupa musi zapewniać odporność na warunki zewnętrzne. Dopuszcza się wykończenie z surowego aluminium, anodowanie, malowanie proszkowe w kolorze RAL albo inne zabezpieczenie powierzchniowe, jeżeli jest zgodne z wymaganiami środowiskowymi lokalizacji i uzgodnieniami z Zamawiającym lub zarządcą terenu. W przypadku lokalizacji reprezentacyjnych, miejskich albo wymagających dostosowania wizualnego, Zamawiający może wymagać malowania proszkowego w uzgodnionym kolorze RAL.

Generalny Wykonawca musi wykonać obliczenia albo przedstawić dokumenty producenta potwierdzające nośność, stateczność i przydatność słupa do montażu zaplanowanego zestawu kamer oraz osprzętu. Dokumentacja musi uwzględniać wysokość montażu, liczbę i masę kamer, sposób montażu, obciążenia wiatrem, lokalne warunki terenowe oraz sposób posadowienia.

Generalny Wykonawca musi wykonać montaż słupa zgodnie z dokumentacją projektową, dokumentacją producenta, zasadami wiedzy technicznej, przepisami BHP oraz wymaganiami właściciela lub zarządcy terenu. Po montażu słup musi zostać wypionowany, trwale zamocowany, oznakowany i sprawdzony pod kątem stabilności, bezpieczeństwa, ciągłości uziemienia, poprawności prowadzenia przewodów oraz gotowości do montażu kamer.

Odbiór słupa kamerowego musi obejmować co najmniej:

1) sprawdzenie zgodności wysokości i konstrukcji słupa z wymaganiami;
2) sprawdzenie sposobu posadowienia i mocowania do fundamentu;
3) sprawdzenie pionowości i stabilności konstrukcji;
4) sprawdzenie zabezpieczenia antykorozyjnego;
5) sprawdzenie prowadzenia i zabezpieczenia okablowania;
6) sprawdzenie wykonania uziemienia i połączeń wyrównawczych;
7) sprawdzenie możliwości bezpiecznego montażu i serwisu kamer;
8) sprawdzenie montażu osprzętu kamerowego;
9) sprawdzenie zastosowania zabezpieczeń przed ptactwem, jeżeli są wymagane;
10) sprawdzenie kompletności dokumentacji technicznej i powykonawczej.

Dokumentacja powykonawcza punktu kamerowego ze słupem musi zawierać co najmniej:

1) lokalizację słupa;
2) wysokość słupa;
3) typ i model zastosowanej konstrukcji;
4) materiał wykonania;
5) sposób wykończenia powierzchni;
6) opis fundamentu i sposobu kotwienia;
7) opis prowadzenia przewodów;
8) opis uziemienia i ochrony przepięciowej;
9) wykaz zamontowanych kamer i osprzętu;
10) dokumentację fotograficzną po montażu;
11) protokół odbioru;
12) instrukcję eksploatacji i serwisu;
13) dokumenty gwarancyjne;

14) karty katalogowe i deklaracje producenta.

1.2.8.3. Wymagania techniczne dla szaf teletechnicznych typu zewnętrznego

Szafy teletechniczne typu zewnętrznego stanowią element terenowej infrastruktury technicznej systemu RIS, przeznaczony do instalacji, zasilania, zabezpieczenia, integracji, monitorowania i eksploatacji urządzeń teleinformatycznych, radiokomunikacyjnych, transmisyjnych, sterujących, pomiarowych, zasilających i zabezpieczających w lokalizacjach terenowych systemu RIS.

Generalny Wykonawca zobowiązany jest do zaprojektowania, dostarczenia, montażu, wyposażenia, konfiguracji, uruchomienia, przetestowania i przekazania do eksploatacji szaf teletechnicznych typu zewnętrznego, odpowiednich dla funkcji danej lokalizacji oraz rodzaju urządzeń instalowanych w danej lokalizacji. Dobór szafy, jej wyposażenia, sposobu montażu, zasilania, zabezpieczeń, monitoringu, wentylacji, ogrzewania, uziemienia, ochrony przepięciowej i powiązań kablowych musi zostać uzgodniony z Zamawiającym i zaakceptowany w dokumentacji projektowej.

Szafy teletechniczne muszą zapewniać bezpieczną całoroczną eksploatację urządzeń w warunkach zewnętrznych, w szczególności w lokalizacjach wieżowych, mostowych, hydrotechnicznych, słupowych, terenowych oraz innych lokalizacjach wskazanych w PFU i dokumentach branżowych. Szafy muszą być dostosowane do pracy w warunkach zmiennych temperatur, wilgotności, opadów, promieniowania UV, zapylenia, oblodzenia, oddziaływania wiatru, drgań, korozji, okresowego zawilgocenia oraz innych czynników środowiskowych właściwych dla Odrzańskiej Drogi Wodnej.

Szafy teletechniczne muszą być dedykowane do użytku zewnętrznego. Minimalne wymagania konstrukcyjne dla szaf obejmują:

1) szerokość nie mniejszą niż 800 mm;
2) głębokość nie mniejszą niż 800 mm;
3) stopień ochrony obudowy nie niższy niż IP55;
4) odporność mechaniczna obudowy nie niższa niż IK10;
5) konstrukcję odporną na korozję i przystosowaną do całorocznej pracy zewnętrznej;
6) możliwość uporządkowanego prowadzenia okablowania zasilającego, sygnałowego, transmisyjnego, światłowodowego, antenowego i ochronnego;
7) możliwość montażu urządzeń w standardzie RACK 19”;
8) możliwość montażu urządzeń na szynie DIN NS 35 zgodnej z EN 60715;
9) możliwość montażu dedykowanych szyn, uchwytów albo paneli dla ochronników torów antenowych, torów sygnałowych, torów transmisyjnych i torów zasilających;
10) możliwość wykonania skutecznego uziemienia, połączeń wyrównawczych i ochrony przepięciowej;
11) możliwość bezpiecznego dostępu serwisowego do wszystkich urządzeń i połączeń.

Wysokość użytkowa szafy musi być dobrana do funkcji lokalizacji, liczby urządzeń, rodzaju urządzeń, wymaganych odstępów montażowych, sposobu chłodzenia, organizacji okablowania oraz rezerwy rozwojowej. Wymaga się, aby:

1) w lokalizacjach wieżowych stosować szafy o wysokości użytkowej co najmniej 42U;
2) w pozostałych lokalizjach stosować szafy o wysokości użytkowej co najmniej 15U;
3) w przypadku lokalizacji o większej liczbie urządzeń, większej liczbie torów antenowych, większych wymaganiach transmisyjnych, większej liczbie kamer, czujników albo urządzeń zasilania rezerwowego, Generalny Wykonawca zastosował szafę o większej wysokości albo większej pojemności montażowej.

W lokalizacjach, w których szafa będzie montowana na fundamencie albo odrębnej konstrukcji nośnej, należy stosować szafy dwudrzwiowe, umożliwiające dostęp serwisowy co najmniej od strony przedniej i tylnej. W lokalizacjach, w których szafa będzie instalowana poprzez mocowanie do ściany tylnej albo do konstrukcji uniemożliwiającej dostęp od tyłu, dopuszcza się stosowanie szaf jednodrzwiowych, pod warunkiem zapewnienia pełnego dostępu serwisowego do wszystkich urządzeń, zabezpieczeń, listew, szyn, połączeń i okablowania.

Drzwi szaf muszą być zamykane na zamek patentowy. System zamknięcia powinien być jednokluczowy i wspólny dla wszystkich lokalizacji, chyba że Zamawiający wskaże inny model zarządzania dostępem. Zastosowany system zamknięcia musi utrudniać dostęp osobom postronnym i zapewniać możliwość kontrolowanego dostępu dla uprawnionych służb Zamawiającego, Generalnego Wykonawcy oraz podmiotów utrzymaniowych działających na rzecz Zamawiającego.

W zależności od możliwości w miejscu instalacji montaż szafy musi być zrealizowany w sposób utrudniający dostęp osobom postronnym. Dotyczy to w szczególności lokalizacji ogólnodostępnych, mostowych, hydrotechnicznych, terenowych i słupowych. Sposób posadowienia albo zamocowania szafy musi ograniczać ryzyko nieuprawnionego otwarcia, uszkodzenia mechanicznego, podważenia, przewrócenia, odłączenia przewodów, zalania, zasypania, korozji, kradzieży albo aktów wandalizmu.

Konstrukcja oraz wymiary szafy muszą umożliwiać łatwy dostęp do każdego urządzenia, modułu, zabezpieczenia, złącza, listwy, ochronnika, patch panelu, przełącznicy, zasilacza, UPS, listwy zasilającej, licznika energii, modułu monitoringu, modułu kontroli dostępu oraz do całości okablowania. Nie dopuszcza się takiego rozmieszczenia urządzeń, które utrudniałoby diagnostykę, wymianę, konfigurację, pomiary, serwis albo kontrolę poprawności połączeń.

Głębokość szaf musi umożliwiać montaż w tylnej części szafy komponentów odpowiedzialnych za ochronę torów antenowych, torów sygnałowych, torów transmisyjnych, torów zasilających i innych torów wprowadzanych do szafy. Rozmieszczenie elementów ochrony przepięciowej, odgromowej, uziemiającej i filtracyjnej musi zapewniać krótkie, uporządkowane i skuteczne połączenia ochronne oraz możliwość kontroli i wymiany tych elementów.

Montaż urządzeń w szafie musi być wykonany w sposób profesjonalny, uporządkowany, trwały i identyfikowalny. Wymaga się stosowania szyn RACK 19”, szyn DIN NS 35 zgodnych z EN

60715, dedykowanych szyn montażowych dla zabezpieczeń torów antenowych i sygnałowych, półek, prowadnic, uchwytów, wsporników, organizerów kabli, przepustów, dławnic, paneli porządkujących, opisów kabli i oznaczeń urządzeń. Wszystkie komponenty stanowiące wyposażenie szafy muszą być dostarczone wraz z uchwytami, półkami, adapterami, mocowaniami albo innymi elementami umożliwiającymi ich prawidłowy montaż.

Szafy teletechniczne muszą być wyposażone co najmniej w:

1) system monitorowania środowiska pracy szafy umożliwiający zdalny dostęp;
2) system kontroli dostępu z możliwością zdalnej dezaktywacji dostępu oraz obsługą karty dostępowej;
3) sygnalizator świetlny powiązany z systemem kontroli dostępu albo alarmami technicznymi;
4) czujnik otwarcia drzwi;
5) czujniki temperatury i wilgotności;
6) automatyczny system wentylacji;
7) system grzewczy;
8) higrostat, termostat, higrotermę albo równoważne urządzenie automatyki środowiskowej;
9) instalację elektryczną szafy;
10) jeden albo dwa zasilacze bezprzerwowe, zależnie od wymagań dostępności danej lokalizacji;
11) zasilacze bezprzerwowe umożliwiające zdalny dostęp, zdalny monitoring stanu pracy, alarmów i parametrów zasilania;
12) zarządzalną listwę zasilającą z modułem zarządzania i monitoringu zasilania umożliwiającym zdalny dostęp;
13) licznik zużycia energii elektrycznej umożliwiający zdalny dostęp;
14) elementy ochrony przepięciowej dla torów zasilających;
15) elementy konstrukcyjne dla elementy ochrony przepięciowej i odgromowej dla torów antenowych, sygnałowych, transmisyjnych i sterujących;
16) listwy uziemiające i połączenia wyrównawcze;
17) przełącznice, patch panele, panele krosowe, organizery i oznakowanie kabli;
18) oświetlenie serwisowe wnętrza szafy;
19) dokumentację lokalizacyjną i schemat połączeń umieszczony w sposób uzgodniony z Zamawiającym albo dostępny w dokumentacji eksploatacyjnej.

System wentylacji i system grzewczy muszą zapewniać warunki pracy urządzeń znajdujących się w szafie zgodnie z deklaracjami producentów tych urządzeń, zarówno w okresie letnim, jak i zimowym. Bilans cieplny szafy musi uwzględniać rzeczywisty pobór mocy urządzeń, nasłonecznienie, temperaturę zewnętrzną, szczelność obudowy, pracę urządzeń transmisyjnych, pracę radiotelefonów, pracę urządzeń rejestrujących, pracę routerów, modemów, przełączników,

sterowników, UPS, liczników, systemów monitoringu, systemów kontroli dostępu oraz urządzeń pomocniczych.

Wentylacja, grzanie, układ odprowadzania kondensatu, filtry, kratki, przepusty i dławnice muszą być dobrane tak, aby nie pogarszać wymaganego stopnia ochrony IP i nie powodować wnikania wody, pyłu, owadów, gryzoni albo zanieczyszczeń do wnętrza szafy. Filtry wentylacyjne muszą być dostępne do okresowej kontroli i wymiany, a procedura ich utrzymania musi zostać opisana w dokumentacji eksploatacyjnej.

Instalacja elektryczna szafy musi być wykonana zgodnie z obowiązującymi przepisami, normami, wymaganiami producentów urządzeń oraz dokumentacją projektową. Musi obejmować co najmniej zabezpieczenia nadprądowe, ochronę przeciwporażeniową, ochronę przepięciową, rozłącznik albo inny element umożliwiający bezpieczne odłączenie zasilania, listwy zasilające, połączenia ochronne, połączenia wyrównawcze, oznakowanie obwodów i przewodów oraz możliwość wykonania pomiarów odbiorczych i okresowych.

Generalny Wykonawca zobowiązany jest w imieniu Zamawiającego podjąć wszystkie niezbędne działania w celu doprowadzenia zasilania do szafy teletechnicznej i urządzeń zainstalowanych w danej lokalizacji. Obowiązek ten obejmuje w szczególności przygotowanie dokumentacji projektowej, uzyskanie warunków przyłączenia, uzgodnień, zgód, pozwoleń, wykonanie przyłącza albo zasilania lokalnego, wykonanie rozliczeń formalnych, montaż zabezpieczeń, liczników, tras kablowych, pomiarów i protokołów wymaganych do bezpiecznego użytkowania instalacji.

Zasilanie szafy musi zostać zaprojektowane na podstawie bilansu energetycznego lokalizacji. Bilans musi obejmować co najmniej urządzenia radiokomunikacyjne, transmisyjne, CCTV, czujniki hydrologiczne, sensory meteorologiczne, lokalne komponenty akwizycji danych, routery, modemy, przełączniki, zabezpieczenia, systemy monitoringu, kontrolę dostępu, wentylację, grzanie, oświetlenie serwisowe, UPS, listwy zasilające oraz rezerwę rozwojową.

Zasilacze bezprzerwowe muszą zapewniać podtrzymanie pracy urządzeń w czasie wymaganym dla danej lokalizacji, wynikającym z architektury systemu RIS, znaczenia lokalizacji, wymagań ciągłości działania, wymagań transmisyjnych i bilansu energetycznego. W lokalizacjach krytycznych, w tym lokalizacjach wieżowych oraz lokalizacjach z urządzeniami VHF/AIS/DGNSS, CCTV, sensorami lub urządzeniami transmisyjnymi o znaczeniu podstawowym dla działania systemu RIS, należy rozważyć zastosowanie dwóch zasilaczy bezprzerwowych albo innego rozwiązania zapewniającego redundancję zasilania.

Zarządzalna listwa zasilająca musi umożliwiać co najmniej zdalny monitoring stanu zasilania, zdalny odczyt parametrów, rejestrację zdarzeń zasilania oraz zdalne zarządzanie wybranymi gniazdami albo obwodami, jeżeli jest to wymagane dla diagnostyki i utrzymania urządzeń. Licznik energii elektrycznej musi umożliwiać zdalny odczyt zużycia energii oraz przekazywanie danych do systemu monitorowania i zarządzania zasobami systemu RIS.

System monitorowania środowiska pracy szafy musi umożliwiać zdalny odczyt co najmniej temperatury, wilgotności, stanu drzwi, alarmu otwarcia, statusu zasilania, statusu wentylacji, statusu ogrzewania, statusu UPS, statusu listwy zasilającej, statusu licznika energii, alarmu przekroczenia progów środowiskowych oraz alarmu utraty komunikacji z urządzeniem monitorującym. Wymagane jest definiowanie progów alarmowych oraz przekazywanie zdarzeń do systemu monitorowania i zarządzania zasobami systemu RIS.

System kontroli dostępu do szafy musi umożliwiać kontrolowane otwieranie szafy przez osoby uprawnione, rejestrację zdarzeń dostępu, sygnalizację nieuprawnionego otwarcia, możliwość zdalnej dezaktywacji uprawnienia, obsługę kart dostępowych albo innego mechanizmu identyfikacji zaakceptowanego przez Zamawiającego oraz integrację z systemem monitorowania i zarządzania zasobami systemu RIS. Zdarzenia kontroli dostępu muszą być rejestrowane i możliwe do późniejszej analizy.

Wszystkie komponenty szafy objęte funkcją zdalnego dostępu muszą zostać włączone do systemu monitorowania i zarządzania zasobami systemu RIS. Dotyczy to w szczególności systemu monitorowania środowiska, kontroli dostępu, UPS, listwy zasilającej, licznika energii, urządzeń transmisyjnych, routerów, modemów, przełączników, lokalnych komponentów akwizycji danych, urządzeń zabezpieczeń, systemów wentylacji, ogrzewania i innych urządzeń wyposażonych w interfejs zarządzający.

Szafy muszą umożliwiać bezpieczne wprowadzenie i zakończenie przewodów zasilających, przewodów sygnałowych, przewodów transmisyjnych, kabli antenowych, światłowodów, przewodów sterujących, przewodów ochronnych i przewodów uziemiających. Wszystkie wejścia kablowe muszą być wykonane z wykorzystaniem przepustów, dławnic, rur osłonowych, kanałów kablowych albo innych elementów zapewniających szczelność, trwałość, odporność mechaniczną, odporność na promieniowanie UV, ochronę przed wodą, lodem, owadami, gryzoniami i dostępem osób nieuprawnionych.

W przypadku lokalizacji mostowych oraz lokalizacji słupów kamerowych szafy nie mogą być instalowane w miejscach, w których dolna część szafy znajdowałaby się poniżej najwyższego znanego poziomu wody z okresu występowania powodzi. Generalny Wykonawca zobowiązany jest zweryfikować lokalne dane dotyczące zagrożenia powodziowego, historycznych stanów wody, warunków hydrologicznych, wymagań zarządcy obiektu oraz ryzyka zalania i uwzględnić je w projekcie posadowienia szafy.

W przypadku instalowania szaf przy obiektach wieżowych szafa musi zostać zamontowana na konstrukcji nośnej na fundamencie wieży zapewniającej, że dolna część szafy będzie znajdowała się powyżej najwyższego znanego poziomu wody z okresu występowania powodzi, chyba że analiza lokalizacji, warunki hydrologiczne i uzgodnienia z Zamawiającym wykażą brak takiego ryzyka. Jeżeli najwyższy znany poziom wody z okresu powodzi jest niższy niż wysokość górnej płaszczyzny fundamentu wieży, szafa musi zostać zainstalowana na konstrukcji nośnej umożliwiającej łatwe doprowadzenie wszystkich instalacji kończących się w szafie oraz bezpieczne prowadzenie kabli pomiędzy szafą a wieżą. Konstrukcja nośna szafy powinna umożliwiać jej wypoziomowanie.

Rysunek 1: Przykładowa konstrukcja nośna szafy wraz z podestem (Lokalizacja Świerkocin)

Rysunek 2: Przykładowa konstrukcja nośna szafy wraz z systemem poziomowania (Lokalizacja Świerkocin)

W zależności od wysokości konstrukcji nośnej Generalny Wykonawca musi zaprojektować i wykonać system schodów, stopni, podestu albo innego rozwiązania umożliwiającego bezpieczny dostęp do przodu szafy i wykonywanie czynności serwisowych. Rozwiązanie to musi

spełniać wymagania BHP, zapewniać stabilne dojście serwisowe, nie powodować ryzyka poślizgnięcia albo upadku, być odporne na warunki zewnętrzne i nie utrudniać eksploatacji lokalizacji.

Szafa oraz jej podstawa, fundament, konstrukcja nośna, kanały kablowe, przepusty, schody, podesty i elementy dostępowe muszą być zaprojektowane jako kompletna lokalna infrastruktura techniczna. Rozwiązanie musi zapewniać ochronę przed wodą opadową, wodą rozbryzgową, okresowym podtopieniem, śniegiem, lodem, zanieczyszczeniami, korozją, uszkodzeniami mechanicznymi oraz dostępem osób nieuprawnionych.

Szafy teletechniczne muszą być uziemione i objęte połączeniami wyrównawczymi. Uziemienie szafy musi być skoordynowane z uziemieniem wieży, słupa, konstrukcji wsporczej, instalacji odgromowej, ochronników przepięciowych, torów antenowych, przewodów ekranowanych, urządzeń zasilania i urządzeń transmisyjnych. Dokumentacja powykonawcza musi zawierać schemat uziemienia, schemat połączeń wyrównawczych oraz wyniki wymaganych pomiarów.

Ochrona przepięciowa szafy musi obejmować wszystkie tory, które tego wymagają ze względu na charakter lokalizacji i rodzaj urządzeń, w szczególności tory zasilające, tory antenowe, tory sygnałowe, tory transmisyjne, tory sterujące oraz przewody wprowadzane z urządzeń zewnętrznych. Ochronniki przepięciowe muszą być dobrane do rodzaju toru, parametrów pracy, poziomu narażenia na przepięcia, wymagań producentów urządzeń oraz projektu ochrony odgromowej.

Organizacja okablowania w szafie musi zapewniać separację kabli zasilających, sygnałowych, antenowych, transmisyjnych, światłowodowych i ochronnych, jeżeli jest to wymagane ze względów bezpieczeństwa, kompatybilności elektromagnetycznej albo parametrów transmisyjnych. Kable muszą być opisane po obu stronach, prowadzone w organizerach, mocowane w sposób niepowodujący uszkodzeń, z zachowaniem promieni gięcia i umożliwieniem późniejszej kontroli.

Szafa teletechniczna musi być oznaczona tabliczką informacyjną z danymi teleadresowymi właściciela, oznaczeniem lokalizacji, numerem szafy albo innym identyfikatorem uzgodnionym z Zamawiającym. Treść, format, trwałość i miejsce montażu tabliczki muszą zostać zatwierdzone przez Zamawiającego. Oznakowanie musi być odporne na warunki zewnętrzne, promieniowanie UV, wilgoć i uszkodzenia mechaniczne.

Na obszarze aktualnego działania systemu RIS Zamawiający eksploatuje w szafach teletechnicznych typu zewnętrznego rozwiązania obejmujące w szczególności: system monitoringu parametrów środowiskowych i kontroli dostępu BKT EMS EC335 wraz z kompletem czujników, grzałkę BKT TC4 Tajfun 400 W / 230 VAC, higrotermę BKT EFT 012, system wentylacji z filtrem BKT, licznik energii elektrycznej Carlo Gavazzi EM24 DI oraz zarządzalną listwę dystrybucyjną 19” BKT IPD1000 8xDIN944, DIN49441.

Informacja ta ma charakter opisu stanu istniejącego oraz punktu odniesienia dla zachowania ciągłości eksploatacyjnej, sposobu monitorowania, organizacji utrzymania, integracji z systemem monitorowania i zarządzania zasobami systemu RIS, a także dla zapewnienia spójności funkcjonalnej i serwisowej nowych lokalizacji z lokalizacjami już eksploatowanymi przez Zamawiającego.

Wskazanie powyższych producentów i modeli nie oznacza obowiązku zastosowania urządzeń tych samych producentów ani ograniczenia konkurencji. Generalny Wykonawca może zastosować rozwiązania równoważne funkcjonalnie, technicznie, eksploatacyjnie i integracyjnie, pod warunkiem, że zapewnią one co najmniej taki sam zakres funkcji, możliwość zdalnego monitorowania i zarządzania, integrację z systemem RIS, odpowiednią trwałość środowiskową, dostępność serwisową oraz akceptację Zamawiającego na etapie dokumentacji projektowej.

Generalny Wykonawca zobowiązany jest uwzględnić szafy teletechniczne w dokumentacji projektowej, wykonawczej, powykonawczej, konfiguracyjnej, eksploatacyjnej i odbiorowej. Dokumentacja musi obejmować co najmniej lokalizację szafy, sposób posadowienia albo mocowania, typ i wymiary szafy, wysokość użytkową, zestawienie wyposażenia, bilans energetyczny, bilans cieplny, schemat instalacji elektrycznej, schemat zasilania rezerwowego, schemat uziemienia, schemat ochrony przepięciowej, schemat połączeń transmisyjnych, schemat organizacji okablowania, wykaz adresów i parametrów zdalnego zarządzania, progi alarmowe oraz procedury utrzymania.

Przed dostawą i montażem szaf Generalny Wykonawca zobowiązany jest przedstawić Zamawiającemu do akceptacji karty katalogowe, rysunki montażowe, schematy wyposażenia, bilanse energetyczne, bilanse cieplne, sposób posadowienia, sposób ochrony przed zalaniem, sposób prowadzenia kabli, sposób uziemienia, sposób monitorowania, sposób kontroli dostępu oraz sposób integracji z systemem monitorowania i zarządzania zasobami systemu RIS.

Odbiór szaf teletechnicznych typu zewnętrznego musi obejmować co najmniej:

1) weryfikację zgodności lokalizacji i sposobu montażu z dokumentacją projektową;
2) weryfikację wymiarów, wysokości użytkowej, stopnia ochrony IP i odporności IK;
3) weryfikację sposobu posadowienia albo zamocowania szafy;
4) weryfikację zabezpieczenia przed dostępem osób nieuprawnionych;
5) weryfikację zabezpieczenia przed zalaniem, w tym wysokości montażu względem danych powodziowych, jeżeli dotyczy;
6) weryfikację wyposażenia wewnętrznego szafy;
7) weryfikację poprawności montażu urządzeń RACK 19”, DIN NS 35 i elementów ochrony torów;
8) weryfikację instalacji elektrycznej i zabezpieczeń;
9) weryfikację działania UPS, listwy zasilającej i licznika energii;
10) weryfikację działania wentylacji, ogrzewania i automatyki środowiskowej;
11) weryfikację działania systemu monitoringu środowiskowego;
12) weryfikację działania systemu kontroli dostępu, czujnika otwarcia i sygnalizacji;
13) weryfikację integracji komponentów z systemem monitorowania i zarządzania zasobami systemu RIS;
14) weryfikację poprawności uziemienia, połączeń wyrównawczych i ochrony przepięciowej;
15) weryfikację poprawności prowadzenia, oznakowania i zabezpieczenia okablowania;

16) wykonanie wymaganych pomiarów elektrycznych, pomiarów uziemienia i testów funkcjonalnych;
17) weryfikację kompletności dokumentacji powykonawczej i eksploatacyjnej.

Generalny Wykonawca zobowiązany jest w okresie realizacji przedmiotu zamówienia oraz w okresie gwarancji wykonywać wymagane przeglądy, kontrole, czynności konserwacyjne i serwisowe szaf teletechnicznych oraz ich wyposażenia. Zakres ten obejmuje co najmniej kontrolę stanu obudowy, zamków, zawiasów, uszczelnień, filtrów, wentylatorów, grzałek, higroterm, instalacji elektrycznej, UPS, listwy zasilającej, licznika energii, systemu monitoringu środowiskowego, kontroli dostępu, ochronników przepięciowych, uziemienia, połączeń wyrównawczych, okablowania oraz stanu mocowania szafy.

W przypadku stwierdzenia uszkodzenia, nieszczelności, korozji, zalania, przegrzewania, nadmiernej wilgotności, awarii wentylacji, awarii ogrzewania, awarii UPS, awarii kontroli dostępu, awarii monitoringu, uszkodzenia ochronników, poluzowania połączeń, uszkodzenia kabli albo innej nieprawidłowości wpływającej na bezpieczeństwo lub pracę urządzeń systemu RIS, Generalny Wykonawca zobowiązany jest niezwłocznie podjąć działania naprawcze, zabezpieczające albo korygujące.

Wszystkie szafy teletechniczne typu zewnętrznego muszą zostać przekazane do eksploatacji jako kompletne, wyposażone, skonfigurowane, oznakowane, zintegrowane i przetestowane elementy lokalizacji terenowych systemu RIS, wraz z dokumentacją, protokołami odbioru, protokołami pomiarów, schematami połączeń, danymi dostępowymi, procedurami eksploatacyjnymi i dokumentami gwarancyjnymi.

1.2.8.4. Wymagania techniczne dla konstrukcji wsporczych

Konstrukcje wsporcze należy rozumieć jako wszystkie elementy konstrukcyjne, montażowe i pomocnicze służące do posadowienia, wyniesienia, zamocowania, ustawienia, stabilizacji albo zabezpieczenia urządzeń systemu RIS, które nie stanowią samodzielnych obiektów wieżowych ani słupów kamerowych opisanych w odrębnych podrozdziałach PFU. Konstrukcje wsporcze obejmują w szczególności wysięgniki, uchwyty, ramy, konsole, obejmy, adaptery, konstrukcje rurowe, konstrukcje kratowe, wsporniki antenowe, wsporniki kamerowe, wsporniki czujników, konstrukcje pod urządzenia transmisyjne, elementy mocowania torów antenowych, elementy mocowania okablowania oraz inne elementy montażowe niezbędne do realizacji infrastruktury terenowej systemu RIS.

Konstrukcje wsporcze muszą umożliwiać bezpieczny, trwały i stabilny montaż urządzeń systemu RIS, w szczególności kamer obserwacyjnych i dozorowych, czujników hydrologicznych, sensorów meteorologicznych, anten transmisyjnych, anten VHF, anten AIS, anten DGNSS/GNSS, elementów torów antenowych, elementów instalacji kablowych, elementów monitoringu technicznego, urządzeń pomocniczych oraz osprzętu niezbędnego do pracy poszczególnych podsystemów.

Konstrukcje wsporcze mogą być instalowane w szczególności na obiektach mostowych, obiektach hydrotechnicznych, obiektach wieżowych, słupach kamerowych, elewacjach,

balustradach technicznych, pomostach, galeriach, elementach konstrukcyjnych obiektów istniejących oraz innych obiektach lub konstrukcjach zaakceptowanych w dokumentacji projektowej. Każdorazowo miejsce, sposób i zakres montażu konstrukcji wsporczej muszą zostać zweryfikowane przez Generalnego Wykonawcę i zaakceptowane przez Zamawiającego, a w przypadkach wymaganych również przez właściciela albo zarządcę obiektu.

Generalny Wykonawca zobowiązany jest dobrać rodzaj, geometrię, materiał, sposób mocowania i parametry konstrukcji wsporczej do funkcji danego urządzenia, warunków lokalizacyjnych, obciążeń użytkowych, obciążeń środowiskowych, wymagań producentów urządzeń, wymagań eksploatacyjnych, wymagań bezpieczeństwa oraz wymagań właściwego zarządcy obiektu. Nie dopuszcza się stosowania konstrukcji przypadkowych, tymczasowych, niedostosowanych do pracy zewnętrznej albo nieobjętych dokumentacją projektową.

Konstrukcje wsporcze muszą zostać zaprojektowane i wykonane z uwzględnieniem co najmniej:

1) rodzaju, masy, wymiarów, powierzchni czynnej i sposobu pracy urządzeń montowanych na konstrukcji;
2) obciążeń stałych, użytkowych, serwisowych, montażowych, wiatrowych, śniegowych, oblodzeniowych, dynamicznych i drganiowych;
3) wpływu konstrukcji wsporczej na obiekt, do którego jest mocowana;
4) wymagań producentów urządzeń w zakresie sposobu montażu, dopuszczalnych drgań, dopuszczalnych odchyłek, minimalnych odległości, pola widzenia, kierunku pracy anteny albo czujnika oraz dostępu serwisowego;
5) wymagań separacji antenowej, kompatybilności elektromagnetycznej, ochrony odgromowej, uziemienia i ochrony przepięciowej;
6) wymagań dotyczących prowadzenia kabli, torów antenowych, przewodów sygnałowych, przewodów zasilających, przewodów sterujących, przewodów uziemiających i światłowodów;
7) warunków terenowych, hydrologicznych, środowiskowych i eksploatacyjnych danej lokalizacji;
8) możliwości bezpiecznego montażu, kontroli, konserwacji, naprawy, regulacji i wymiany urządzeń;
9) wymagań BHP, pracy na wysokości, dostępu serwisowego i zabezpieczenia przed dostępem osób nieuprawnionych;
10) wymagań formalnoprawnych, uzgodnień, zgód, warunków technicznych i ograniczeń wskazanych przez właściciela albo zarządcę obiektu.

Konstrukcje wsporcze muszą być wykonane z materiałów zapewniających wymaganą nośność, sztywność, trwałość, odporność na korozję oraz odporność na warunki środowiskowe właściwe dla lokalizacji nadwodnych, mostowych, hydrotechnicznych i terenowych. Preferowane jest stosowanie stali ocynkowanej ogniowo, stali nierdzewnej, aluminium konstrukcyjnego albo innych materiałów odpornych na warunki zewnętrzne, pod warunkiem wykazania ich równoważnej albo wyższej trwałości, nośności i odporności środowiskowej.

Wszystkie elementy stalowe konstrukcji wsporczych muszą być zabezpieczone antykorozyjnie w sposób dostosowany do klasy korozyjności środowiska danej lokalizacji. Zabezpieczenie antykorozyjne musi obejmować zarówno zasadnicze elementy nośne, jak i elementy mocujące, obejmy, śruby, nakrętki, podkładki, kotwy, wsporniki, płytki montażowe, adaptery, kształtowniki, rury, prowadnice i inne elementy pomocnicze. Dobór systemu ochrony antykorozyjnej musi zostać opisany w dokumentacji projektowej.

Konstrukcje wsporcze montowane na obiektach mostowych, hydrotechnicznych, drogowych, kolejowych albo innych obiektach istniejących nie mogą pogarszać stanu technicznego tych obiektów, naruszać ich nośności, stateczności, trwałości, szczelności, zabezpieczeń antykorozyjnych, odwodnienia, funkcji użytkowej ani bezpieczeństwa eksploatacji. Wszelkie ingerencje w elementy konstrukcyjne, osłonowe, balustrady, pomosty, elewacje, nawierzchnie, podpory, dźwigary albo elementy wyposażenia obiektu muszą zostać zaprojektowane, uzgodnione i wykonane zgodnie z wymaganiami właściwego zarządcy.

W przypadku montażu konstrukcji wsporczych na obiektach mostowych Generalny Wykonawca zobowiązany jest uwzględnić w szczególności oddziaływania drgań, przemieszczeń, odkształceń termicznych, obciążeń komunikacyjnych, prac utrzymaniowych, ograniczeń dostępu oraz wymagań dotyczących zachowania prześwitu pionowego i poziomego. Konstrukcje wsporcze oraz montowane na nich urządzenia nie mogą ograniczać skrajni żeglugowej, prześwitu pod mostem, szerokości użytkowej przęsła, widoczności znaków nawigacyjnych, dostępu do elementów obiektu ani bezpieczeństwa ruchu.

Konstrukcje wsporcze przeznaczone dla kamer muszą zapewniać stabilność obrazu, brak nadmiernych drgań, zachowanie wymaganego pola widzenia, możliwość ustawienia właściwego kierunku obserwacji, możliwość regulacji położenia kamery oraz możliwość późniejszego serwisu. Konstrukcja nie może powodować przesłonięcia obszaru obserwacji, wprowadzania niepożądanych odbić, drgań albo zakłóceń wpływających na jakość obrazu i skuteczność monitoringu wizyjnego.

Konstrukcje wsporcze przeznaczone dla czujników hydrologicznych muszą zapewniać stabilne i trwałe położenie czujnika względem lustra wody, brak przenoszenia drgań mogących zafałszować pomiar, odporność na odkształcenia wynikające ze zmian temperatury oraz możliwość ustawienia czujnika w sposób zapewniający poprawną geometrię pomiaru. Konstrukcja nie może ograniczać prześwitu pionowego ani szerokości pomiędzy podporami albo prowadnicami mostu i nie może powodować lokalnych zakłóceń pomiaru.

Konstrukcje wsporcze przeznaczone dla sensorów meteorologicznych muszą zapewniać montaż w miejscu możliwie reprezentatywnym dla pomiaru warunków atmosferycznych, z ograniczeniem wpływu przesłon terenowych, elementów konstrukcyjnych, źródeł ciepła, odbić, zawirowań powietrza i innych czynników mogących wpływać na wynik pomiaru. Konstrukcja musi zapewniać właściwą ekspozycję sensora, stabilność montażu, dostęp serwisowy oraz prowadzenie przewodów bez ryzyka uszkodzenia.

Konstrukcje wsporcze przeznaczone dla anten i torów antenowych muszą zapewniać zachowanie wymaganej wysokości montażu, kierunku, polaryzacji, separacji antenowej, stabilności mechanicznej, odporności na wiatr i oblodzenie oraz możliwości prowadzenia kabli antenowych zgodnie z wymaganiami producentów urządzeń i dokumentacją projektową.

Konstrukcje te muszą być skoordynowane z instalacją odgromową, uziemieniem, połączeniami wyrównawczymi i ochroną przepięciową.

Konstrukcje wsporcze przeznaczone dla urządzeń transmisyjnych oraz anten transmisji danych muszą umożliwiać uzyskanie wymaganych parametrów transmisyjnych, w szczególności zachowanie kierunku pracy anteny, stabilności ustawienia, warunków propagacyjnych, wymagań widoczności radiowej, dostępu serwisowego oraz bezpiecznego prowadzenia kabli i przewodów zasilających. W przypadku anten kierunkowych konstrukcja wsporcza musi zapewniać możliwość precyzyjnej regulacji azymutu i elewacji oraz trwałego zablokowania ustawienia po uruchomieniu.

Konstrukcje wsporcze muszą umożliwiać uporządkowane, trwałe i identyfikowalne prowadzenie przewodów, kabli, torów antenowych, światłowodów oraz przewodów ochronnych. Trasy kablowe prowadzone po konstrukcjach wsporczych muszą być zabezpieczone przed uszkodzeniami mechanicznymi, promieniowaniem UV, wilgocią, wodą, lodem, korozją, drganiami, nadmiernym zginaniem, niekontrolowanymi naprężeniami oraz dostępem osób nieuprawnionych. Należy zachować wymagane promienie gięcia, separację przewodów oraz oznakowanie kabli.

Wszelkie przepusty, przejścia kablowe, otwory, obejmy, mocowania i elementy prowadzenia kabli muszą być wykonane w sposób trwały, szczelny, uporządkowany i możliwy do kontroli. Nie dopuszcza się prowadzenia przewodów luzem, bez zabezpieczenia, bez oznakowania albo w sposób utrudniający dostęp serwisowy, powodujący ryzyko uszkodzenia izolacji, pogorszenia parametrów transmisyjnych albo naruszenia bezpieczeństwa osób wykonujących czynności eksploatacyjne.

Konstrukcje wsporcze muszą być objęte systemem uziemienia, połączeń wyrównawczych, ochrony odgromowej i ochrony przepięciowej w zakresie wynikającym z rodzaju urządzeń, miejsca montażu, dokumentacji projektowej, analizy ryzyka oraz wymagań producentów urządzeń. Konstrukcje metalowe, wsporniki antenowe, maszty pomocnicze, elementy prowadzenia kabli, ekrany przewodów, elementy torów antenowych i szafy powiązane z konstrukcją muszą zostać ujęte w dokumentacji połączeń wyrównawczych.

Konstrukcje wsporcze muszą być projektowane w sposób umożliwiający bezpieczny montaż i późniejszą obsługę urządzeń. Jeżeli czynności serwisowe wymagają dostępu na wysokości albo dostępu z obiektu mostowego, wieżowego, hydrotechnicznego albo innego obiektu technicznego, Generalny Wykonawca zobowiązany jest przewidzieć rozwiązania zapewniające bezpieczny dostęp, możliwość stosowania środków ochrony indywidualnej, punkty asekuracyjne, procedury serwisowe albo inne rozwiązania wymagane przepisami BHP i warunkami zarządcy obiektu.

Konstrukcje wsporcze muszą być zaprojektowane w sposób umożliwiający demontaż, wymianę, regulację albo serwis urządzeń bez konieczności niszczenia podstawowych elementów konstrukcji wsporczej, obiektu, do którego jest ona mocowana, oraz tras kablowych. Jeżeli demontaż albo wymiana urządzenia może wymagać czasowego demontażu elementu konstrukcji wsporczej, sposób ten musi zostać opisany w dokumentacji eksploatacyjnej.

W przypadku stosowania konstrukcji wsporczych na istniejących obiektach Generalny Wykonawca zobowiązany jest wykonać inwentaryzację i ocenę możliwości montażu. Ocena musi obejmować co najmniej stan techniczny miejsca mocowania, dostępność montażową,

dostępność serwisową, możliwe kolizje z istniejącą infrastrukturą, ograniczenia eksploatacyjne, wymagania zarządcy, wpływ na obiekt oraz możliwość prowadzenia kabli i uziemień.

Generalny Wykonawca zobowiązany jest uzyskać wszystkie wymagane zgody, uzgodnienia, opinie, warunki techniczne i pozwolenia dotyczące montażu konstrukcji wsporczych na obiektach lub nieruchomościach nienależących do Zamawiającego. Dotyczy to w szczególności obiektów mostowych, drogowych, kolejowych, hydrotechnicznych, obiektów PGW Wody Polskie, obiektów jednostek samorządu terytorialnego, obiektów podmiotów prywatnych oraz innych obiektów wykorzystywanych jako platforma nośna infrastruktury RIS.

Konstrukcje wsporcze muszą być oznakowane w sposób umożliwiający ich identyfikację w dokumentacji eksploatacyjnej systemu RIS. Oznakowanie powinno umożliwiać powiązanie konstrukcji z lokalizacją, urządzeniem, trasą kablową, dokumentacją projektową, dokumentacją powykonawczą i procedurami utrzymaniowymi. Oznakowanie nie może pogarszać bezpieczeństwa, trwałości ani estetyki obiektu.

Generalny Wykonawca zobowiązany jest opracować dokumentację projektową konstrukcji wsporczych, obejmującą co najmniej opis funkcji konstrukcji, lokalizację, rysunki montażowe, sposób mocowania, zestawienie materiałów, sposób zabezpieczenia antykorozyjnego, obliczenia albo dobór konstrukcyjny, schemat prowadzenia przewodów, opis uziemienia, opis ochrony odgromowej i przepięciowej, opis dostępu serwisowego oraz wymagane uzgodnienia z właścicielem albo zarządcą obiektu.

Dokumentacja projektowa konstrukcji wsporczych musi być spójna z dokumentacją branżową dla systemu CCTV, systemu VHF/AIS/DGNSS, sieci połączeń transmisyjnych, czujników hydrologicznych, sensorów meteorologicznych, zasilania, uziemienia, ochrony odgromowej, tras kablowych, szaf teletechnicznych oraz dokumentacją powykonawczą i eksploatacyjną systemu RIS.

Przed wykonaniem konstrukcji wsporczej Generalny Wykonawca zobowiązany jest przedstawić Zamawiającemu do akceptacji rozwiązanie projektowe, w tym sposób mocowania, sposób zabezpieczenia antykorozyjnego, sposób prowadzenia kabli, sposób uziemienia, zakres ingerencji w obiekt oraz wymagane uzgodnienia. Wykonanie konstrukcji bez akceptacji dokumentacji projektowej następuje na ryzyko Generalnego Wykonawcy.

Odbiór konstrukcji wsporczych musi obejmować co najmniej:

1) weryfikację zgodności lokalizacji z dokumentacją projektową;
2) weryfikację zgodności typu, materiału i geometrii konstrukcji z dokumentacją projektową;
3) weryfikację sposobu mocowania do obiektu albo podłoża;
4) weryfikację jakości wykonania zabezpieczenia antykorozyjnego;
5) weryfikację kompletności połączeń śrubowych, kotew, obejm, uchwytów i elementów montażowych;
6) weryfikację stabilności i sztywności konstrukcji;
7) weryfikację poprawności montażu urządzeń;
8) weryfikację możliwości regulacji, serwisu i wymiany urządzeń;
9) weryfikację poprawności prowadzenia przewodów, torów antenowych i tras kablowych;

10) weryfikację uziemienia, połączeń wyrównawczych, ochrony odgromowej i ochrony przepięciowej;
11) weryfikację braku kolizji z funkcją obiektu, skrajnią, prześwitem, dostępem serwisowym i istniejącą infrastrukturą;
12) weryfikację dokumentacji fotograficznej, protokołów montażu, protokołów pomiarowych i dokumentacji powykonawczej.

Dokumentacja powykonawcza konstrukcji wsporczych musi zawierać co najmniej:

1) lokalizację konstrukcji;
2) opis funkcji konstrukcji;
3) typ i model zastosowanej konstrukcji albo opis rozwiązania indywidualnego;
4) materiał wykonania;
5) sposób zabezpieczenia antykorozyjnego;
6) sposób mocowania do obiektu albo podłoża;
7) wykaz zamontowanych urządzeń;
8) opis prowadzenia przewodów i tras kablowych;
9) opis uziemienia, połączeń wyrównawczych i ochrony przepięciowej;
10) dokumentację fotograficzną po montażu;
11) protokoły montażu i odbioru;
12) protokoły pomiarów, jeżeli są wymagane;
13) instrukcję eksploatacji i serwisu;
14) dokumenty gwarancyjne;
15) karty katalogowe, deklaracje zgodności, atesty albo inne dokumenty potwierdzające parametry zastosowanych materiałów i elementów.

Generalny Wykonawca zobowiązany jest w okresie realizacji przedmiotu zamówienia oraz w okresie gwarancji wykonywać wymagane przeglądy, kontrole, czynności konserwacyjne i serwisowe konstrukcji wsporczych oraz ich połączeń z obiektami. Zakres ten obejmuje w szczególności kontrolę stanu technicznego, stabilności, połączeń śrubowych, kotew, mocowań, zabezpieczeń antykorozyjnych, tras kablowych, uziemienia, ochrony przepięciowej oraz elementów zamontowanych na konstrukcji.

W przypadku stwierdzenia uszkodzenia, korozji, poluzowania mocowań, odkształcenia, nadmiernych drgań, pogorszenia stabilności, utraty ustawienia urządzenia, uszkodzenia tras kablowych albo innej nieprawidłowości mogącej wpływać na bezpieczeństwo lub prawidłową pracę urządzeń systemu RIS, Generalny Wykonawca zobowiązany jest niezwłocznie podjąć działania naprawcze, zabezpieczające albo korygujące, zgodnie z wymaganiami Zamawiającego i warunkami gwarancji.

Wszystkie konstrukcje wsporcze muszą zostać przekazane do eksploatacji jako element kompletnej lokalizacji terenowej systemu RIS, wraz z zamontowanymi urządzeniami, okablowaniem, uziemieniem, ochroną przepięciową, dokumentacją, oznakowaniem, protokołami odbioru oraz procedurami eksploatacyjnymi.

1.2.9. Wymagania dla nowych zasilaczy awaryjnych oraz wymiany zasilaczy awaryjnych lub zasobników energii

Rozdział określa wymagania Zamawiającego dotyczące zasilania awaryjnego urządzeń systemu RIS instalowanych w nowych lokalizacjach terenowych oraz w istniejących lokalizacjach objętych modernizacją, odtworzeniem albo wymianą elementów infrastruktury technicznej. Wymagania obejmują zarówno dostawę i uruchomienie nowych zasilaczy awaryjnych wraz z kompatybilnymi zasobnikami energii, jak również wymianę zasilaczy awaryjnych lub modułów bateryjnych w lokalizacjach, w których eksploatowane obecnie rozwiązania wymagają zastąpienia, odtworzenia albo przywrócenia pełnej sprawności eksploatacyjnej.

Zasilacze awaryjne stanowią element infrastruktury krytycznej lokalizacji terenowych systemu RIS. Ich zadaniem jest zapewnienie ciągłości pracy urządzeń teleinformatycznych, radiokomunikacyjnych, transmisyjnych, pomiarowych, obserwacyjnych, diagnostycznych, monitoringu technicznego, kontroli dostępu oraz lokalnych komponentów akwizycji danych w przypadku zaniku, zakłócenia albo pogorszenia jakości zasilania podstawowego.

Wymagania określone w niniejszym rozdziale należy stosować do lokalizacji nowych oraz do lokalizacji istniejących, w których przewidziano wymianę obecnie eksploatowanych zasilaczy awaryjnych, wymianę modułów bateryjnych, dostosowanie układu zasilania szafy teletechnicznej, montaż przełączników zasilania awaryjnego, integrację układu zasilania z systemem monitorowania i zarządzania zasobami systemu RIS albo inne czynności modernizacyjne związane z zapewnieniem ciągłości zasilania urządzeń terenowych.

Zakres wymagań obejmuje w szczególności:

1) wymagania dla nowych zasilaczy awaryjnych i współpracujących z nimi zasobników energii;
2) wymagania dla wymiany zasilaczy awaryjnych wycofywanych z eksploatacji;
3) wymagania dla wymiany modułów bateryjnych w istniejących zasilaczach awaryjnych;
4) wymagania dotyczące montażu, konfiguracji, uruchomienia i integracji układów zasilania awaryjnego;
5) wymagania dotyczące monitorowania stanu pracy zasilacza, zasobnika energii, alarmów, trybu pracy i parametrów zasilania;
6) wymagania dotyczące dokumentacji projektowej, powykonawczej i eksploatacyjnej;
7) wymagania dotyczące testów odbiorowych, pomiarów, przeglądów, serwisu i utrzymania w okresie realizacji oraz w okresie gwarancji.

Dobór zasilacza awaryjnego, liczby zasobników energii, sposobu montażu, sposobu włączenia do instalacji elektrycznej, sposobu monitorowania oraz wymaganego czasu podtrzymania musi wynikać z bilansu energetycznego danej lokalizacji. Bilans ten musi uwzględniać wszystkie urządzenia zasilane z układu awaryjnego, w tym urządzenia transmisji danych, urządzenia radiokomunikacyjne VHF/AIS/DGNSS, urządzenia CCTV, czujniki hydrologiczne, czujniki meteorologiczne, lokalne komponenty akwizycji danych, urządzenia monitoringu środowiskowego, kontroli dostępu, zabezpieczeń, zdalnego zarządzania oraz pozostałe urządzenia przewidziane do pracy w danej szafie teletechnicznej.

Układy zasilania awaryjnego muszą być projektowane i wykonywane jako integralny element lokalizacji terenowej systemu RIS, a nie jako samodzielne urządzenie zasilające oderwane od pozostałej infrastruktury. Oznacza to konieczność ich powiązania z instalacją elektryczną, szafą teletechniczną typu zewnętrznego, ochroną przeciwporażeniową, ochroną przepięciową, uziemieniem, połączeniami wyrównawczymi, monitoringiem technicznym, dokumentacją eksploatacyjną, procedurami serwisowymi oraz systemem monitorowania i zarządzania zasobami systemu RIS.

W przypadku lokalizacji istniejących Generalny Wykonawca zobowiązany jest przed rozpoczęciem prac zweryfikować aktualny stan techniczny układu zasilania, stan zasilaczy awaryjnych, stan zasobników energii, sposób podłączenia urządzeń, obciążenie układu, stan zabezpieczeń, sposób uziemienia, dostępność miejsca montażowego, sposób prowadzenia przewodów, integrację z monitoringiem oraz wpływ planowanych prac na ciągłość działania systemu RIS. Wyniki tej weryfikacji muszą zostać uwzględnione w dokumentacji projektowej oraz w planie realizacji prac.

Prace związane z wymianą, montażem albo rekonfiguracją zasilaczy awaryjnych i zasobników energii muszą być prowadzone w sposób minimalizujący ryzyko przerwy w działaniu urządzeń systemu RIS, utraty danych, utraty komunikacji, uszkodzenia urządzeń, naruszenia bezpieczeństwa elektrycznego albo utraty monitorowania danej lokalizacji. Jeżeli prace wymagają czasowego wyłączenia zasilania, muszą zostać zaplanowane, uzgodnione z Zamawiającym i wykonane w zaakceptowanym oknie serwisowym.

Dostarczane zasilacze awaryjne, zasobniki energii, przełączniki, elementy montażowe, zabezpieczenia, przewody, urządzenia pośredniczące w komunikacji oraz pozostałe komponenty układu zasilania awaryjnego muszą być nowe, pełnowartościowe, zgodne z wymaganiami producentów, właściwe dla pracy w szafach teletechnicznych typu zewnętrznego oraz dostosowane do warunków środowiskowych, elektrycznych i eksploatacyjnych danej lokalizacji.

Wszystkie układy zasilania awaryjnego objęte niniejszym rozdziałem muszą zostać przekazane do eksploatacji jako kompletne, zamontowane, skonfigurowane, opisane, przetestowane, udokumentowane i zintegrowane elementy systemu RIS. Szczegółowe wymagania dla nowych zasilaczy awaryjnych określono w podrozdziale 1.2.9.1, natomiast wymagania dotyczące wymiany modułów bateryjnych w istniejących zasilaczach awaryjnych określono w podrozdziale 1.2.9.2.

1.2.9.1. Opis wymagań dla zasilacza awaryjnego

Generalny Wykonawca zobowiązany jest dostarczyć, zamontować, skonfigurować, uruchomić, zintegrować, przetestować i przekazać do eksploatacji zasilacze awaryjne wraz zasobnikami energii przeznaczone do podtrzymania pracy urządzeń systemu RIS w nowych lokalizacjach terenowych oraz w istniejących lokalizacjach modernizowanych, w których przewidziano wymianę wycofywanych z eksploatacji zasilaczy awaryjnych.

Zasilacze awaryjne muszą być przeznaczone do pracy w szafach teletechnicznych typu zewnętrznego oraz do zasilania urządzeń teleinformatycznych, radiokomunikacyjnych, transmisyjnych, pomiarowych, monitoringu technicznego, kontroli dostępu, lokalnych komponentów akwizycji danych, urządzeń CCTV oraz innych urządzeń systemu RIS, zgodnie z bilansem energetycznym danej lokalizacji.

Zasilacz awaryjny musi spełniać co najmniej następujące wymagania elektryczne:

1) znamionowe napięcie wejściowe: 230 V AC;
2) częstotliwość wejściowa: 50/60 Hz ± 3 Hz, z automatycznym wykrywaniem częstotliwości;
3) zakres napięcia wejściowego rozumiany jako różnica pomiędzy minimalną i maksymalną dopuszczalną wartością napięcia wejściowego: nie mniejszy niż 80 V AC;
4) znamionowe napięcie wyjściowe: 230 V AC;
5) znamionowy prąd wyjściowy: nie mniejszy niż 2,2 A;
6) moc znamionowa czynna: nie mniejsza niż 400 W;
7) moc pozorna: dobrana odpowiednio do mocy czynnej i charakteru zasilanych odbiorników;
8) kształt napięcia wyjściowego w trybie pracy bateryjnej odpowiedni dla zasilania urządzeń elektronicznych instalowanych w lokalizacjach systemu RIS;
9) czas przełączenia na pracę bateryjną niewpływający na ciągłość pracy urządzeń zasilanych z zasilacza awaryjnego;
10) możliwość pracy z zewnętrznym, kompatybilnym zasobnikiem energii.

Zasilacz awaryjny musi spełniać co najmniej następujące wymagania środowiskowe i montażowe:

1) stopień ochrony obudowy: co najmniej IP20;
2) praca w temperaturze otoczenia co najmniej w zakresie od -20°C do +40°C;
3) maksymalna dopuszczalna wilgotność względna powietrza w czasie pracy: nie mniej niż 95%, bez kondensacji;
4) montaż na szynie DIN NS 35 zgodnej z EN 60715;
5) konstrukcja przystosowana do montażu w szafie teletechnicznej typu zewnętrznego;
6) możliwość uporządkowanego prowadzenia przewodów zasilających, sygnałowych, komunikacyjnych i przewodów do zasobnika energii;

7) możliwość bezpiecznej obsługi, diagnostyki, wymiany i kontroli w warunkach eksploatacji terenowej.

Zasilacz awaryjny musi posiadać interfejs komunikacyjny albo zestaw wyjść sygnalizacyjnych umożliwiających monitorowanie stanu urządzenia oraz kontrolę podstawowych trybów pracy. Wymaga się, aby do systemu monitorowania i zarządzania zasobami systemu RIS były przekazywane co najmniej następujące informacje i funkcje:

1) praca w trybie zasilania sieciowego;
2) praca w trybie zasilania bateryjnego;
3) stan naładowania zasobnika energii;
4) stan gotowości zasilacza awaryjnego;
5) alarm awarii albo nieprawidłowej pracy zasilacza;
6) alarm niskiego poziomu energii w zasobniku;
7) informacja o stanie zasobnika energii albo konieczności jego wymiany, jeżeli funkcja taka jest dostępna dla zastosowanego rozwiązania;
8) zdalne włączenie, wyłączenie albo restart zasilania na wyjściu, jeżeli jest to wymagane dla danej lokalizacji i możliwe przy zachowaniu bezpieczeństwa pracy urządzeń.

Jeżeli oferowany zasilacz awaryjny nie posiada natywnego interfejsu Ethernet/IP, Generalny Wykonawca zobowiązany jest zapewnić konwersję sygnalizacji kontrolnej, statusowej i alarmowej do standardu umożliwiającego integrację z systemem monitorowania i zarządzania zasobami systemu RIS. Konwersja musi obejmować wszystkie wymagane sygnały stanu, alarmy i funkcje sterujące przewidziane dla danej lokalizacji.

Zasilacz awaryjny musi współpracować z zasobnikiem energii spełniającym co najmniej następujące wymagania:

1) zasobnik energii musi być kompatybilny z oferowanym zasilaczem awaryjnym;
2) zasobnik energii musi być wykonany jako zewnętrzny moduł albo zestaw modułów zintegrowanych funkcjonalnie z zasilaczem awaryjnym;
3) zasobnik energii musi zapewniać podtrzymanie pracy zestawu zasilania awaryjnego przez okres nie krótszy niż 10 minut przy obciążeniu 400 W;
4) zasobnik energii musi być przystosowany do pracy w temperaturze otoczenia co najmniej w zakresie od -20°C do +40°C;
5) maksymalna dopuszczalna wilgotność względna powietrza w czasie pracy zasobnika energii musi wynosić nie mniej niż 95%;
6) stopień ochrony obudowy zasobnika energii musi wynosić co najmniej IP20;
7) zasobnik energii musi być przystosowany do montażu w szafie teletechnicznej typu zewnętrznego albo na płycie montażowej / szynie / półce przewidzianej w dokumentacji projektowej;

8) zasobnik energii musi umożliwiać bezpieczne podłączenie, eksploatację, diagnostykę, kontrolę i wymianę w warunkach eksploatacyjnych lokalizacji terenowej.

W celu potwierdzenia spełnienia wymagań dotyczących czasu podtrzymania Generalny Wykonawca zobowiązany jest dostarczyć wraz z Dokumentacją projektową dokument wystawiony przez producenta albo autoryzowanego przedstawiciela producenta, potwierdzający czas pracy oferowanego zestawu zasilacza awaryjnego i zasobnika energii przy obciążeniu 400 W przez okres co najmniej 10 minut. Dokumentem potwierdzającym może być w szczególności karta katalogowa, tabela czasu pracy, wykres czasu pracy, raport doboru albo inny dokument techniczny jednoznacznie odnoszący się do oferowanej konfiguracji.

Zasilacz awaryjny oraz zasobnik energii muszą zostać włączone do systemu monitorowania i zarządzania zasobami systemu RIS. Integracja musi umożliwiać co najmniej zdalny podgląd stanu pracy, sygnalizację alarmów, rejestrację zdarzeń, informację o pracy z zasilania bateryjnego, informację o powrocie zasilania sieciowego oraz informację o stanie zasobnika energii.

Generalny Wykonawca zobowiązany jest zapewnić, aby zasilacz awaryjny, zasobnik energii oraz urządzenia pośredniczące w monitorowaniu i konwersji sygnałów były zainstalowane w sposób uporządkowany, trwały, bezpieczny i zgodny z wymaganiami producentów. Montaż musi uwzględniać wymagane odstępy wentylacyjne, dopuszczalną temperaturę pracy, dostęp serwisowy, ochronę przed przypadkowym odłączeniem, oznakowanie przewodów, ochronę przeciwporażeniową, ochronę przepięciową, uziemienie oraz połączenia wyrównawcze.

Instalacja zasilacza awaryjnego musi być poprzedzona opracowaniem bilansu energetycznego dla danej lokalizacji. Bilans musi obejmować wszystkie urządzenia zasilane z układu awaryjnego, w szczególności urządzenia transmisyjne, routery, modemy, przełączniki, urządzenia VHF/AIS/DGNSS, urządzenia CCTV, czujniki hydrologiczne, sensory meteorologiczne, lokalne komponenty akwizycji danych, urządzenia monitoringu środowiskowego, kontroli dostępu, listwy zasilające, liczniki energii oraz inne urządzenia przewidziane w danej szafie teletechnicznej.

Zasilacz awaryjny musi być objęty testami odbiorowymi. Testy muszą obejmować co najmniej:

1) weryfikację zgodności modelu, parametrów i konfiguracji z dokumentacją projektową;
2) weryfikację poprawności montażu na szynie DIN NS 35 zgodnej z EN 60715;
3) weryfikację poprawności podłączenia zasilania wejściowego, wyjściowego i zasobnika energii;
4) weryfikację pracy w trybie zasilania sieciowego;
5) weryfikację przejścia do trybu zasilania bateryjnego;
6) weryfikację powrotu do trybu zasilania sieciowego;
7) weryfikację przekazywania sygnałów stanu i alarmów do systemu monitorowania i zarządzania zasobami systemu RIS;
8) weryfikację funkcji zdalnego włączenia, wyłączenia albo restartu zasilania na wyjściu, jeżeli została przewidziana dla danej lokalizacji;

9) weryfikację czasu podtrzymania przy obciążeniu odpowiadającym konfiguracji danej lokalizacji;
10) weryfikację dokumentów producenta potwierdzających wymagany czas podtrzymania przy obciążeniu 400 W przez co najmniej 10 minut.

Generalny Wykonawca zobowiązany jest przekazać Zamawiającemu dokumentację powykonawczą i eksploatacyjną układu zasilania awaryjnego, obejmującą co najmniej schemat zasilania, schemat połączeń sygnałowych i komunikacyjnych, bilans energetyczny, dobór zasobnika energii, opis integracji z systemem monitorowania, wykaz parametrów konfiguracyjnych, instrukcję eksploatacji, instrukcję wymiany zasobnika energii, zalecenia dotyczące przeglądów, protokoły testów, protokoły pomiarów oraz dokumenty gwarancyjne.

W okresie realizacji przedmiotu zamówienia oraz w okresie gwarancji Generalny Wykonawca zobowiązany jest wykonywać przeglądy, kontrole, testy i czynności serwisowe zasilaczy awaryjnych oraz zasobników energii zgodnie z wymaganiami producentów, dokumentacją eksploatacyjną, Szczegółowym Planem Przeglądów i Aktualizacji oraz wymaganiami Zamawiającego. Zakres ten obejmuje w szczególności kontrolę stanu zasilacza, zasobnika energii, połączeń, alarmów, komunikacji, parametrów pracy, czasu podtrzymania oraz zdolności do przejścia w tryb zasilania bateryjnego.

1.2.9.2. Opis wymagań dla wymiany modułu bateryjnego UPS-BAT/VRLA-WTR/24DC/13AH w zasilaczu awaryjnym QUINT-UPS/1AC/1AC/500VA

Przedmiotem czynności serwisowej jest wymiana modułu bateryjnego współpracującego z zasilaczem awaryjnym QUINT-UPS/1AC/1AC/500VA, numer katalogowy 2320270, na nowy moduł typu UPS-BAT/VRLA-WTR/24DC/13AH, numer katalogowy 2320416. Zasilacz ten jest jednostką UPS z technologią IQ, przeznaczoną do pracy w instalacjach 120/230 V AC, zapewniającą na wyjściu czystą sinusoidę oraz moc 400 W / 500 VA. Producent wskazuje jednocześnie, że urządzenie wymaga do pracy dodatkowego zasobnika energii, a sam układ UPS przekazuje informacje o stanie naładowania, pozostałym czasie podtrzymania oraz przewidywanej żywotności modułu akumulatorowego.

Wymiana powinna być rozumiana nie jako samo mechaniczne zastąpienie jednego elementu drugim, ale jako pełne przywrócenie układowi zasilania awaryjnego zdolności do prawidłowego podtrzymania napięcia oraz do dalszej diagnostyki stanu baterii przez system UPS. Nowy moduł bateryjny musi być fabrycznie nowy, nieużywany i zgodny z wymaganiami producenta urządzenia. Moduł UPS-BAT/VRLA-WTR/24DC/13AH jest przez Phoenix Contact opisany jako zasobnik energii w technologii VRLA-WTR / pure lead AGM, o napięciu 24 V DC i pojemności 13 Ah, wyposażony w funkcję automatycznego wykrywania oraz komunikacji z QUINT UPS-IQ. Producent wskazuje również możliwość beznarzędziowej wymiany oraz stałej komunikacji z UPS w celu monitorowania i inteligentnego zarządzania pracą baterii.

W ramach realizacji zadania należy przyjąć, że wymieniany moduł ma być w pełni kompatybilny z eksploatowanym zasilaczem awaryjnym. Zgodność ta musi obejmować zarówno parametry elektryczne, jak i właściwą współpracę diagnostyczną z technologią IQ zastosowaną w zasilaczu.

Producent modułu wskazuje, że bateria jest przeznaczona do zastosowania z rodzinami QUINT4 DC-UPS, QUINT4 AC-UPS oraz QUINT-UPS, natomiast producent samego zasilacza potwierdza, że urządzenie pracuje z zewnętrznym zasobnikiem energii 24 V DC i obsługuje informacje o stanie modułu bateryjnego w sposób ciągły. Oznacza to, że wykonawca powinien przed montażem potwierdzić zgodność zainstalowanego UPS z dostarczanym modułem nie tylko na poziomie nazwy handlowej, lecz także numeru katalogowego i konfiguracji eksploatowanej w danym obiekcie.

Dostarczone moduły mają zachowywwać wszystkie istotne cechy użytkowe przewidziane przez producenta. Obejmuje to napięcie znamionowe 24 V DC, pojemność 13 Ah, prąd ładowania 5,2 A, napięcie końca ładowania 27,6 V przy 20°C, a także deklarowaną żywotność na poziomie 10–15 lat przy 20°C. Producent podaje również, że moduł osiąga orientacyjny czas podtrzymania 50 minut przy obciążeniu 10 A oraz 10 minut przy 40 A, co stanowi istotny parametr odniesienia przy ocenie stanu pracy po wymianie.

Prace serwisowe powinny zostać wykonane przez personel posiadający odpowiednie kwalifikacje do obsługi urządzeń elektrycznych oraz doświadczenie w pracach przy systemach zasilania gwarantowanego. Wymiana musi zostać przeprowadzona zgodnie z dokumentacją producenta i z zachowaniem warunków montażowych przewidzianych dla tego typu zasobnika energii. Moduł powinien być instalowany poziomo, na płycie montażowej.

Zakres prac Wykonawcy ma obejmować przygotowanie stanowiska, bezpieczne wyłączenie lub przełączenie układu zgodnie z warunkami eksploatacyjnymi obiektu, demontaż zużytego modułu, montaż nowego zasobnika energii, sprawdzenie połączeń, uruchomienie układu UPS oraz weryfikację czy zasilacz prawidłowo rozpoznaje nowy moduł bateryjny. Po zakończeniu montażu należy przeprowadzić test funkcjonalny obejmujący co najmniej ocenę pracy w trybie normalnym, przejście na pracę bateryjną oraz kontrolę podstawowych sygnałów diagnostycznych. Celem tych czynności jest potwierdzenie, że po wymianie układ odzyskał zdolność bezpiecznego podtrzymania zasilania i poprawnego raportowania stanu baterii. Wymóg ten wynika bezpośrednio z faktu, że producent UPS akcentuje funkcję ciągłego raportowania stanu naładowania, czasu podtrzymania i żywotności modułu.

W dokumentacji powykonawczej z wymiany powinno znaleźć się potwierdzenie zastosowanego numeru katalogowego modułu, numer seryjny baterii, data montażu, wynik testu funkcjonalnego oraz potwierdzenie poprawnej współpracy z zasilaczem awaryjnym. Należy również odnotować przewidywany termin kolejnej kontroli eksploatacyjnej. Jest to uzasadnione tym, że producent wyraźnie wskazuje ograniczoną trwałość magazynową modułu i obowiązek jego okresowego doładowywania, jeżeli nie zostanie uruchomiony w odpowiednim czasie. Na opakowaniu producent wskazuje termin, do którego bateria powinna zostać uruchomiona lub doładowana.

Opis wymagań powinien także obejmować obowiązek właściwego zagospodarowania zużytego modułu. Bateria zdemontowana z urządzenia nie może zostać potraktowana jako zwykły odpad komunalny. Producent jednoznacznie wskazuje konieczność postępowania zgodnie z właściwymi przepisami krajowymi dotyczącymi utylizacji baterii i odpadów tego rodzaju. W praktyce oznacza to, że wykonawca powinien odebrać zużyty moduł i przekazać go do dalszego zagospodarowania zgodnie z obowiązującymi wymaganiami środowiskowymi.

Za prawidłowo wykonaną wymianę należy uznać taką realizację, w której zastosowano właściwy i zgodny moduł bateryjny, przeprowadzono montaż zgodnie z warunkami producenta,

potwierdzono poprawne rozpoznanie baterii przez UPS, wykonano test funkcjonalny bez aktywnych błędów oraz przekazano użytkownikowi komplet informacji potwierdzających poprawność wykonanych prac. W sensie eksploatacyjnym rezultat wymiany powinien polegać na odtworzeniu pełnej funkcjonalności układu podtrzymania zasilania oraz przywróceniu możliwości dalszego monitorowania parametrów baterii przez system QUINT UPS z technologią IQ.

1.2.10. Wymagania dla modernizacji serwerowni

1.2.10.1. Przedmiot zadania

Przedmiotem zadania jest zaprojektowanie, wykonanie, wyposażenie, uruchomienie, przetestowanie i przekazanie do eksploatacji zmodernizowanego pomieszczenia serwerowni pełniącej rolę węzła telekomunikacyjnego systemu RIS.

Modernizacja dotyczy pokoju nr 32 zlokalizowanego na parterze budynku siedziby Zamawiającego. Pomieszczenie to pełni funkcję węzła koncentracji dla segmentu sieci LAN oraz infrastruktury telekomunikacyjnej wykorzystywanej do komunikacji z systemem RIS, w tym z lokalizacjami terenowymi systemu informacji rzecznej, urządzeniami transmisyjnymi, urządzeniami sieciowymi oraz pozostałymi elementami infrastruktury komunikacyjnej.

Celem modernizacji jest utworzenie jednego, funkcjonalnie wydzielonego i kompletnego pomieszczenia technicznego przeznaczonego do pracy urządzeń teleinformatycznych, sieciowych, transmisyjnych, bezpieczeństwa i monitoringu technicznego, spełniającego wymagania właściwe dla węzła telekomunikacyjnego systemu RIS.

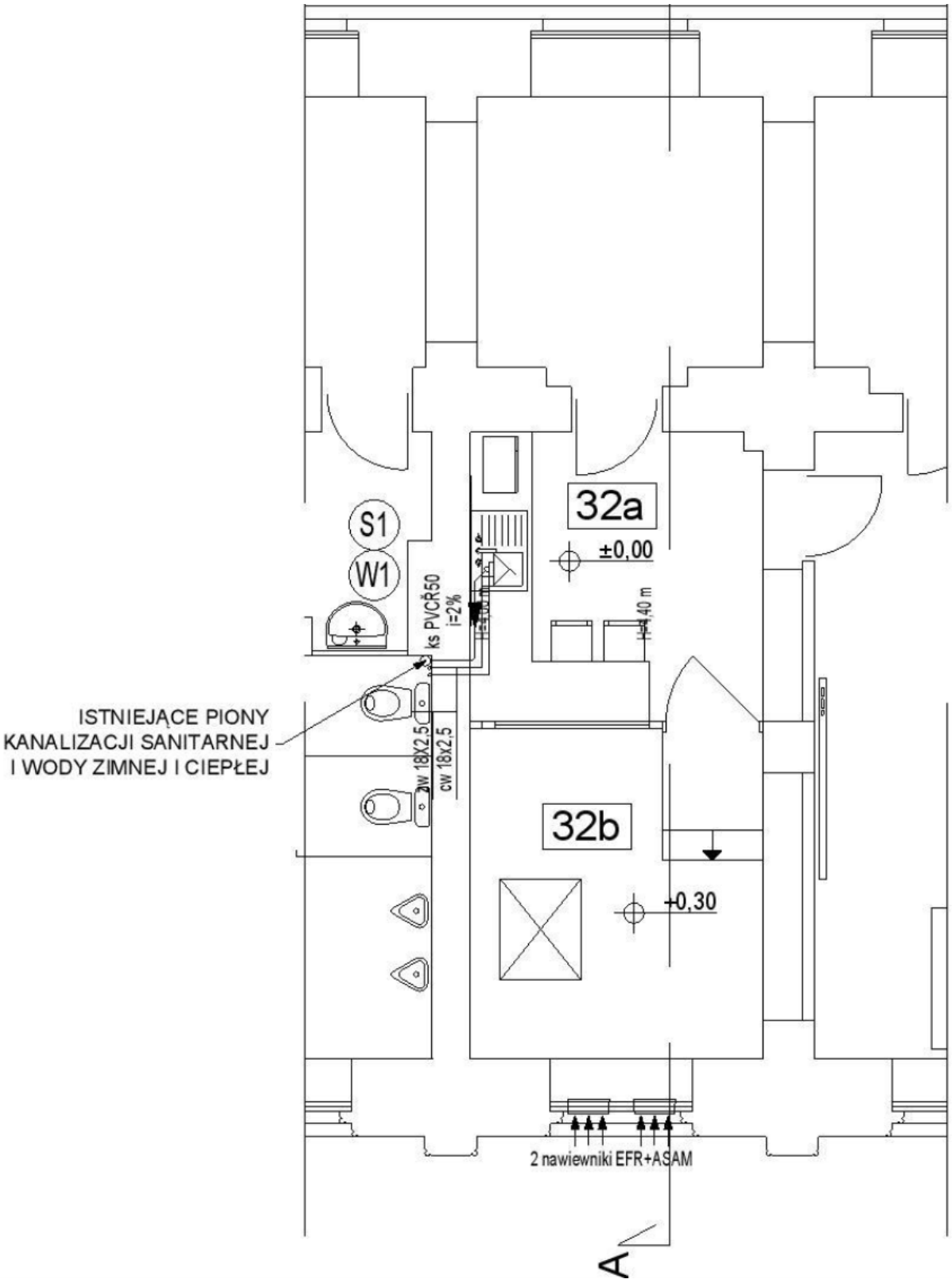
1.2.10.2. Stan istniejący i docelowy układ pomieszczenia

Aktualnie pokój nr 32 składa się z dwóch części funkcjonalnych, tj. pomieszczenia technicznego oraz pomieszczenia serwerowni wyposażonego w podłogę techniczną. W wyniku modernizacji ma powstać jedno pomieszczenie obejmujące cały pokój nr 32, przeznaczone do pełnienia funkcji serwerowni telekomunikacyjnej oraz węzła koncentracji sieci.

Łączna powierzchnia pomieszczenia wynosi 20m^2, a wysokość ok. 4,4 m. W pomieszczeniu technicznym występują przyłącza do istniejącej kanalizacji sanitarnej oraz wody zimnej i ciepłej.

Pomieszczenie techniczne jest obecnie połączone z pokojem nr 31. Przejście pomiędzy pokojem nr 32 a pokojem nr 31 musi zostać zlikwidowane poprzez demontaż drzwi i framugi oraz trwałe zamurowanie otworu. Prace te muszą zostać wykonane w sposób zapewniający właściwą izolację funkcjonalną, bezpieczeństwo fizyczne, odporność ogniową, estetykę wykończenia oraz zgodność z wymaganiami przepisów budowlanych i przeciwpożarowych.

Generalny Wykonawca zobowiązany jest zweryfikować stan istniejący pomieszczenia, w szczególności układ ścian, drzwi, podłogi technicznej, przepustów, tras kablowych, instalacji elektrycznych, instalacji teletechnicznych, wentylacji, klimatyzacji, systemu kontroli dostępu, ochrony przeciwpożarowej, uziemienia, połączeń wyrównawczych oraz istniejących urządzeń teleinformatycznych.



Rysunek 3: Rzut pomieszczenia 32

1.2.10.3. Zakres odpowiedzialności Generalnego Wykonawcy

Generalny Wykonawca zobowiązany jest zrealizować zadanie w formule „zaprojektuj i zbuduj”, obejmującej co najmniej:

1) wykonanie inwentaryzacji stanu istniejącego;
2) analizę istniejących powiązań pomieszczenia z Serwerownią Główną, pokojem nr 31, segmentem sieci LAN, siecią transmisji danych systemu RIS oraz istniejącymi kanałami kablowymi;
3) opracowanie dokumentacji projektowej modernizacji pomieszczenia;
4) uzyskanie wymaganych uzgodnień, opinii i akceptacji Zamawiającego;
5) wykonanie prac rozbiórkowych, budowlanych, instalacyjnych, montażowych, elektrycznych, teletechnicznych, przeciwpożarowych i wykończeniowych;
6) wykonanie nowego toru zasilającego z Serwerowni Głównej;
7) wykonanie dedykowanego kanału kablowego dla toru zasilającego pomiędzy Serwerownią Główną a serwerownią telekomunikacyjną;
8) dostawę, montaż i uruchomienie szaf RACK wraz z systemem precyzyjnego chłodzenia oraz wykonanie klimatyzacji pomieszczenia serwerowni telekomunikacyjnej;
9) dostosowanie albo wykonanie systemu kontroli dostępu;
10) dostosowanie albo wykonanie systemów bezpieczeństwa pożarowego i gaszenia;
11) objęcie pomieszczenia monitoringiem technicznym i zarządzaniem infrastruktury;
12) wykonanie testów, pomiarów, sprawdzeń i odbiorów;
13) opracowanie i przekazanie dokumentacji powykonawczej, konfiguracyjnej, eksploatacyjnej i serwisowej;
14) przeprowadzenie instruktażu lub szkolenia personelu Zamawiającego w zakresie eksploatacji dostarczonych rozwiązań;
15) zapewnienie gwarancji, serwisu i wsparcia zgodnie z wymaganiami PFU i Umowy.

1.2.10.4. Wymagania dotyczące dokumentacji projektowej

Generalny Wykonawca zobowiązany jest opracować dokumentację projektową modernizacji serwerowni telekomunikacyjnej i przedłożyć ją Zamawiającemu do akceptacji przed rozpoczęciem prac wykonawczych.

Dokumentacja projektowa musi obejmować co najmniej:

1) opis stanu istniejącego;
2) opis założeń projektowych;
3) rzut pomieszczenia przed i po modernizacji;
4) układ funkcjonalny pomieszczenia po modernizacji;

5) rozmieszczenie szaf RACK, urządzeń, klimatyzacji precyzyjnej, elementów kontroli dostępu, elementów systemu przeciwpożarowego, elementów monitoringu technicznego, przepustów i tras kablowych;
6) projekt klimatyzacji pomieszczenia,
7) projekt likwidacji przejścia pomiędzy pokojem nr 32 a pokojem nr 31;
8) projekt zasilania serwerowni telekomunikacyjnej z Serwerowni Głównej;
9) projekt rozbudowy rozdzielnicy głównej w Serwerowni Głównej o dedykowany obwód zasilający serwerownię telekomunikacyjną oraz segment sieci LAN, dla którego serwerownia telekomunikacyjna jest węzłem koncentracji;
10) projekt dedykowanego kanału kablowego dla toru zasilającego pomiędzy Serwerownią Główną a serwerownią telekomunikacyjną;
11) opis sposobu prowadzenia toru zasilającego na poziomie -1 oraz przejścia z poziomu -1 na poziom 0 przez pomieszczenie znajdujące się pod serwerownią telekomunikacyjną;
12) analizę wpływu projektowanych tras kablowych na istniejące okablowanie sygnałowe łączące obie serwerownie;
13) projekt połączeń wyrównawczych, uziemienia i ochrony przeciwprzepięciowej;
14) projekt systemu klimatyzacji precyzyjnej;
15) projekt systemu kontroli dostępu oraz jego integracji z istniejącym systemem Zamawiającego;
16) projekt monitoringu technicznego pomieszczenia i infrastruktury;
17) projekt zabezpieczeń przeciwpożarowych i systemu gaszenia;
18) opis etapowania prac i sposobu zachowania ciągłości działania infrastruktury telekomunikacyjnej;
19) plan testów, pomiarów i odbiorów;
20) wykaz urządzeń, materiałów, licencji, elementów montażowych i wyposażenia;
21) analizę ryzyk związanych z realizacją prac w działającym węźle telekomunikacyjnym.

Dokumentacja projektowa musi być spójna z dokumentacją istniejącej Serwerowni Głównej, dokumentacją powykonawczą systemu kontroli dostępu, dokumentacją powykonawczą sieci transmisyjnej RIS, dokumentacją eksploatacyjną systemu RIS oraz pozostałymi dokumentami przekazanymi przez Zamawiającego.

1.2.10.5. Wymagania dotyczące ciągłości działania podczas realizacji prac

Serwerownia telekomunikacyjna pełni rolę węzła komunikacyjnego dla infrastruktury systemu RIS. Generalny Wykonawca zobowiązany jest zaplanować i prowadzić prace w sposób zapewniający ciągłość dostępu do sieci publicznej wykorzystywanej do komunikacji lokalizacji systemu informacji rzecznej oraz infrastruktury w nich zainstalowanej z systemem centralnym.

Generalny Wykonawca zobowiązany jest przed rozpoczęciem prac opracować Plan Zachowania Ciągłości Działania Węzła Telekomunikacyjnego na czas modernizacji. Plan ten musi zostać uzgodniony z Zamawiającym i musi obejmować co najmniej:

1) identyfikację wszystkich usług, urządzeń, połączeń, torów transmisyjnych i zasilających, na które mogą oddziaływać prace modernizacyjne;
2) wskazanie usług krytycznych dla działania systemu RIS;
3) wykaz prac możliwych do wykonania bez przerwy w działaniu;
4) wykaz prac wymagających okna serwisowego;
5) propozycję okien serwisowych i zasad ich uzgadniania z Zamawiającym;
6) sposób czasowego zabezpieczenia albo obejścia połączeń krytycznych;
7) sposób zabezpieczenia istniejącego okablowania sygnałowego i urządzeń czynnych;
8) zasady prowadzenia prac w pobliżu działających urządzeń teleinformatycznych;
9) procedury awaryjne na wypadek utraty łączności, zasilania, dostępu do sieci publicznej albo degradacji parametrów transmisji;
10) osoby odpowiedzialne po stronie Generalnego Wykonawcy za koordynację prac i komunikację z Zamawiającym;
11) sposób dokumentowania przerw planowych, przerw nieplanowych i działań odtworzeniowych;
12) warunki przywrócenia stanu poprzedniego w przypadku niepowodzenia prac.

Żadne prace mogące skutkować przerwą w działaniu usług komunikacyjnych systemu RIS, utratą dostępu do sieci publicznej, degradacją parametrów transmisji, odłączeniem urządzeń aktywnych, odłączeniem zasilania albo zmianą konfiguracji urządzeń sieciowych nie mogą być wykonane bez uprzedniej akceptacji Zamawiającego.

1.2.10.6. Wymagania budowlano-adaptacyjne

Generalny Wykonawca zobowiązany jest wykonać wszystkie prace budowlano-adaptacyjne niezbędne do utworzenia jednego pomieszczenia serwerowni telekomunikacyjnej w obrębie pokoju nr 32.

Zakres prac budowlano-adaptacyjnych obejmuje co najmniej:

1) zabezpieczenie pomieszczenia, urządzeń, tras kablowych i instalacji przed rozpoczęciem prac;
2) demontaż elementów wyposażenia, okładzin, instalacji i zabudów kolidujących z docelowym układem pomieszczenia;
3) demontaż drzwi i framugi w przejściu pomiędzy pokojem nr 32 a pokojem nr 31;
4) zamurowanie przejścia pomiędzy pokojem nr 32 a pokojem nr 31;

5) odtworzenie powierzchni ścian, sufitów i posadzek po wykonanych pracach;
6) dostosowanie istniejącej podłogi technicznej albo wykonanie jej rozbudowy, naprawy, przebudowy lub wymiany w zakresie niezbędnym do uzyskania jednego spójnego pomieszczenia technicznego;
7) wykonanie wymaganych przepustów, przejść instalacyjnych i zabezpieczeń ogniowych;
8) wykonanie wykończenia pomieszczenia właściwego dla pomieszczeń technicznych i serwerowych;
9) wykonanie oznaczeń, opisów technicznych i tablic informacyjnych wymaganych dla bezpiecznej eksploatacji;
10) uporządkowanie i oznaczenie przestrzeni technicznej po zakończeniu prac.

Materiały wykończeniowe zastosowane w pomieszczeniu muszą być trwałe, niepylące, łatwe do utrzymania w czystości, odpowiednie dla pomieszczeń technicznych, spełniać wymagania przeciwpożarowe i nie mogą negatywnie oddziaływać na pracę urządzeń teleinformatycznych.

1.2.10.7. Drzwi, zabezpieczenia fizyczne i dostęp do pomieszczenia

Serwerownia telekomunikacyjna musi stanowić pomieszczenie o kontrolowanym dostępie fizycznym. Generalny Wykonawca zobowiązany jest zweryfikować stan istniejących drzwi do pokoju nr 32 i w razie potrzeby dostosować je albo wymienić, tak aby spełniały wymagania właściwe dla pomieszczeń technicznych i teleinformatycznych.

Drzwi wejściowe do serwerowni telekomunikacyjnej muszą spełniać co najmniej następujące wymagania:

1) umożliwiać integrację z systemem kontroli dostępu Zamawiającego;
2) zapewniać możliwość awaryjnego otwarcia od wewnątrz;
3) być wyposażone w elementy wykonawcze kontroli dostępu właściwe dla przyjętego projektu;
4) zapewniać odpowiedni poziom odporności mechanicznej i bezpieczeństwa fizycznego;
5) spełniać wymagania przeciwpożarowe wynikające z projektu, uzgodnień i obowiązujących przepisów;
6) umożliwiać ewakuację i działanie służb ratowniczych zgodnie z przepisami.

Generalny Wykonawca zobowiązany jest zapewnić, aby wszelkie zmiany w obrębie drzwi, zamków, elektrozaczepów, czytników, przycisków awaryjnych i elementów kontroli dostępu były zgodne z istniejącym systemem Zamawiającego oraz zaakceptowaną dokumentacją projektową.

1.2.10.8. Zasilanie serwerowni telekomunikacyjnej

Serwerownia telekomunikacyjna musi być zasilana z Serwerowni Głównej. Generalny Wykonawca zobowiązany jest rozbudować rozdzielnicę główną w Serwerowni Głównej o dedykowany obwód zasilający serwerownię telekomunikacyjną oraz segment sieci LAN, dla którego serwerownia telekomunikacyjna pełni rolę węzła koncentracji.

Zakres prac dotyczących zasilania obejmuje co najmniej:

1) inwentaryzację istniejącej rozdzielnicy głównej w Serwerowni Głównej;
2) weryfikację dostępnej mocy, rezerwy zasilania, zabezpieczeń, torów zasilania, układu zasilania gwarantowanego i rezerwowego;
3) dobór zabezpieczeń, przekrojów kabli, tras kablowych, przepustów i elementów rozdzielczych;
4) wykonanie dedykowanego obwodu zasilającego serwerownię telekomunikacyjną;
5) wykonanie zasilania urządzeń aktywnych, szaf RACK, systemu chłodzenia precyzyjnego, kontroli dostępu, monitoringu technicznego, systemu przeciwpożarowego i pozostałych urządzeń pomocniczych;
6) wykonanie ochrony przeciwporażeniowej, przeciwprzepięciowej, uziemienia i połączeń wyrównawczych;
7) wykonanie oznaczeń obwodów, zabezpieczeń, kabli, tras i punktów zasilania;
8) wykonanie pomiarów elektrycznych i przekazanie protokołów;
9) aktualizację dokumentacji rozdzielnicy głównej i dokumentacji powykonawczej.

Instalacja zasilająca musi być zaprojektowana i wykonana w sposób zapewniający bezpieczeństwo, niezawodność, możliwość prowadzenia prac serwisowych, czytelność eksploatacyjną oraz możliwość identyfikacji wszystkich obwodów zasilających serwerownię telekomunikacyjną.

1.2.10.9. Dedykowany kanał kablowy dla toru zasilającego

Generalny Wykonawca zobowiązany jest wykonać dedykowany kanał kablowy przeznaczony do poprowadzenia toru zasilającego pomiędzy Serwerownią Główną a serwerownią telekomunikacyjną.

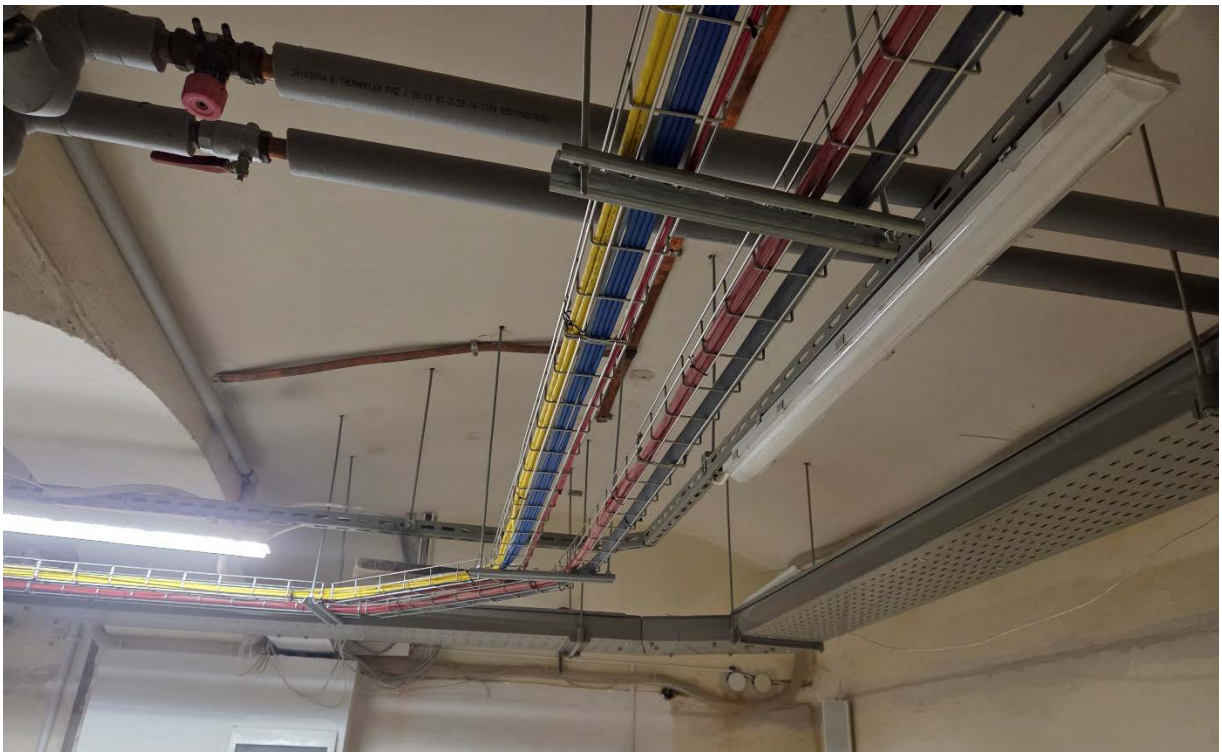
Kanał kablowy musi zostać zaprojektowany i wykonany z uwzględnieniem następujących uwarunkowań:

1) Serwerownia Główna znajduje się na poziomie -1;
2) serwerownia telekomunikacyjna znajduje się na poziomie 0, tj. na parterze budynku;
3) kanały kablowe prowadzone są na poziomie -1;

4) przejście z poziomu -1 na poziom 0 odbywa się przez pomieszczenie znajdujące się pod serwerownią telekomunikacyjną;
5) w ramach pełnego wdrożenia RIS Dolnej Odry obie serwerownie zostały połączone okablowaniem sygnałowym ułożonym w dedykowanych kanałach kablowych;
6) lokalizacja nowego kanału kablowego nie może oddziaływać negatywnie na istniejące okablowanie sygnałowe łączące obie serwerownie;
7) prace nie mogą powodować uszkodzenia, przemieszczenia, przeciążenia, zgniecenia, nadmiernego zagięcia albo rozszczelnienia istniejących torów kablowych;
8) nowy kanał kablowy musi zapewniać wymaganą separację torów zasilających od torów sygnałowych;
9) przejścia przez przegrody budowlane muszą zostać wykonane z zachowaniem wymaganej odporności ogniowej i uszczelnień przeciwpożarowych;
10) przebieg kanału musi zostać jednoznacznie oznaczony i ujęty w dokumentacji powykonawczej.

Generalny Wykonawca zobowiązany jest przed wykonaniem kanału kablowego przedstawić Zamawiającemu projekt trasy, opis technologii wykonania, sposób zabezpieczenia istniejącego okablowania sygnałowego oraz analizę wpływu prac na ciągłość działania systemu RIS.

Rysunek 4: Kanały kablowe łączące pomieszczenia serwerowni



Rysunek 5: Kanały kablowe łączące pomieszczenia serwerowni

1.2.10.10. Szafy RACK i organizacja zabudowy technicznej

W serwerowni telekomunikacyjnej Generalny Wykonawca zobowiązany jest zamontować maksymalnie 3 szafy RACK. Ostateczna liczba szaf, ich rozmieszczenie, wysokość, głębokość, nośność, wyposażenie i sposób organizacji przestrzeni muszą wynikać z dokumentacji projektowej, bilansu urządzeń, wymagań chłodzenia, wymagań zasilania, wymagań prowadzenia okablowania oraz wymagań dostępu serwisowego.

Szafy RACK muszą spełniać co najmniej następujące wymagania:

1) być przeznaczone do montażu urządzeń teleinformatycznych, sieciowych, transmisyjnych, bezpieczeństwa, monitoringu i zasilania pomocniczego;
2) umożliwiać montaż urządzeń w standardzie 19 cali;
3) zapewniać odpowiednią nośność dla planowanego wyposażenia;
4) zapewniać możliwość uporządkowanego prowadzenia kabli zasilających i sygnałowych;
5) umożliwiać montaż listew zasilających, paneli krosowych, organizerów kablowych, przełączników, routerów, urządzeń bezpieczeństwa, urządzeń transmisyjnych i elementów monitoringu;
6) posiadać rozwiązania umożliwiające uziemienie i połączenia wyrównawcze;
7) zapewniać dostęp serwisowy z przodu i z tyłu, o ile pozwalają na to warunki pomieszczenia;
8) być oznaczone w sposób umożliwiający jednoznaczną identyfikację w dokumentacji i systemie monitorowania;

9) być wyposażone w akcesoria niezbędne do prawidłowego montażu i eksploatacji urządzeń;
10) być kompatybilne z przyjętym systemem chłodzenia precyzyjnego.

Rozmieszczenie szaf RACK musi zapewniać możliwość bezpiecznej obsługi serwisowej, wymiany urządzeń, rozbudowy okablowania, kontroli stanu technicznego, prowadzenia pomiarów oraz zachowania wymaganych warunków chłodzenia.

1.2.10.11. Klimatyzacja pomieszczenia oraz system precyzyjnego chłodzenia szaf RACK

Generalny Wykonawca zobowiązany jest zaprojektować, dostarczyć, zamontować, uruchomić, skonfigurować i przekazać do eksploatacji system klimatyzacji pomieszczenia serwerowni telekomunikacyjnej oraz system precyzyjnego chłodzenia szaf RACK.

Systemy chłodzenia muszą zostać zaprojektowane jako rozwiązania wzajemnie skoordynowane, lecz pełniące odrębne funkcje. Klimatyzacja pomieszczenia ma zapewniać utrzymanie wymaganych warunków środowiskowych w całym pomieszczeniu serwerowni telekomunikacyjnej, natomiast system precyzyjnego chłodzenia szaf RACK ma zapewniać lokalne i stabilne warunki pracy urządzeń zainstalowanych w szafach RACK.

Generalny Wykonawca zobowiązany jest opracować bilans cieplny serwerowni telekomunikacyjnej, obejmujący co najmniej:

1) urządzenia planowane do zainstalowania w szafach RACK;
2) urządzenia istniejące, które pozostaną w pomieszczeniu po modernizacji;
3) urządzenia zasilania, transmisji, bezpieczeństwa, monitoringu technicznego i kontroli dostępu;
4) planowaną maksymalną liczbę szaf RACK;
5) zyski ciepła od urządzeń aktywnych, zasilaczy, listew zasilających, UPS, jeżeli zostaną zastosowane oraz pozostałych elementów wyposażenia;
6) zyski ciepła wynikające z warunków budowlanych i lokalizacji pomieszczenia;
7) wymaganą rezerwę chłodniczą na przyszłą rozbudowę;
8) sposób współpracy klimatyzacji pomieszczenia z systemem precyzyjnego chłodzenia szaf RACK.

Bilans cieplny musi zostać przedstawiony Zamawiającemu w dokumentacji projektowej i stanowić podstawę doboru urządzeń klimatyzacyjnych oraz systemu precyzyjnego chłodzenia.

Klimatyzacja pomieszczenia serwerowni telekomunikacyjnej musi spełniać co najmniej następujące wymagania:

1) zapewniać utrzymanie warunków środowiskowych właściwych dla pracy urządzeń teleinformatycznych, sieciowych, transmisyjnych, bezpieczeństwa i monitoringu technicznego;
2) być przeznaczona do pracy ciągłej w pomieszczeniu technicznym;
3) zapewniać utrzymanie temperatury i wilgotności w zakresie dopuszczalnym dla urządzeń zainstalowanych w pomieszczeniu;
4) uwzględniać pracę pomieszczenia jako węzła telekomunikacyjnego systemu RIS;
5) zapewniać rezerwę mocy chłodniczej adekwatną do planowanej rozbudowy wyposażenia pomieszczenia;
6) umożliwiać automatyczną regulację pracy;
7) umożliwiać lokalną i zdalną sygnalizację stanów alarmowych;
8) umożliwiać monitoring podstawowych parametrów pracy;
9) generować alarmy w przypadku awarii, przekroczenia progów temperatury, utraty zasilania, niewłaściwego trybu pracy albo innych stanów nieprawidłowych;
10) być zintegrowana z systemem monitoringu technicznego Zamawiającego albo rozwiązaniem wdrażanym przez Generalnego Wykonawcę;
11) być skoordynowana z systemem przeciwpożarowym, systemem gaszenia, kontrolą dostępu, zasilaniem i układem wentylacji pomieszczenia;
12) umożliwiać prowadzenie przeglądów, konserwacji i czynności serwisowych bez nieuzasadnionego ryzyka dla ciągłości pracy infrastruktury teleinformatycznej;
13) być objęta gwarancją, serwisem i wsparciem producenta przez okres wymagany w PFU i Umowie.

System precyzyjnego chłodzenia szaf RACK musi spełniać co najmniej następujące wymagania:

1) być dostosowany do maksymalnie 3 szaf RACK zainstalowanych w serwerowni telekomunikacyjnej;
2) zapewniać stabilne warunki pracy urządzeń zainstalowanych w szafach RACK;
3) zapewniać lokalne odprowadzanie ciepła z przestrzeni szaf RACK;
4) być dobrany na podstawie bilansu cieplnego urządzeń planowanych do zainstalowania w szafach;
5) współpracować z klimatyzacją pomieszczenia;
6) zapewniać możliwość pracy ciągłej;
7) umożliwiać monitoring parametrów pracy;
8) generować alarmy w przypadku awarii, przekroczenia progów temperatury, utraty zasilania albo innych stanów nieprawidłowych;
9) być zintegrowany z systemem monitoringu technicznego Zamawiającego albo rozwiązaniem wdrażanym przez Generalnego Wykonawcę;
10) umożliwiać prowadzenie przeglądów i czynności serwisowych;

11) być wyposażony w dokumentację techniczną, eksploatacyjną i serwisową;
12) być objęty gwarancją i wsparciem producenta;
13) być zamontowany w sposób nieograniczający dostępu serwisowego do szaf, urządzeń i tras kablowych.

Generalny Wykonawca zobowiązany jest zapewnić, aby klimatyzacja pomieszczenia oraz system precyzyjnego chłodzenia szaf RACK działały w sposób skoordynowany i nie powodowały wzajemnych zakłóceń. W szczególności niedopuszczalne jest zastosowanie rozwiązań powodujących niekontrolowaną cyrkulację powietrza, lokalne przegrzewanie urządzeń, kondensację wilgoci, kolizję z systemem gaszenia, utrudnienie dostępu serwisowego albo negatywny wpływ na istniejące lub projektowane urządzenia teleinformatyczne.

Generalny Wykonawca zobowiązany jest określić w dokumentacji projektowej wymagane parametry pracy systemów chłodzenia, w szczególności:

1) zakładaną temperaturę roboczą pomieszczenia;
2) dopuszczalne progi ostrzegawcze i alarmowe temperatury;
3) wymagany zakres wilgotności, jeżeli wynika to z zastosowanych urządzeń;
4) moc chłodniczą klimatyzacji pomieszczenia;
5) moc chłodniczą systemu precyzyjnego chłodzenia szaf RACK;
6) rezerwę mocy chłodniczej;
7) sposób sterowania i monitorowania;
8) sposób alarmowania;
9) sposób odprowadzenia skroplin;
10) sposób zasilania urządzeń chłodzenia;
11) wymagania dotyczące przeglądów i konserwacji;
12) scenariusze reakcji na awarię klimatyzacji pomieszczenia albo systemu chłodzenia szaf RACK.

Po wykonaniu instalacji Generalny Wykonawca zobowiązany jest przeprowadzić testy działania klimatyzacji pomieszczenia oraz systemu precyzyjnego chłodzenia szaf RACK. Testy muszą obejmować co najmniej uruchomienie urządzeń, weryfikację poprawności pracy, weryfikację odczytu parametrów środowiskowych, weryfikację progów alarmowych, weryfikację przekazywania alarmów do systemu monitoringu technicznego, sprawdzenie odprowadzenia skroplin, sprawdzenie wpływu chłodzenia na pracę szaf RACK oraz potwierdzenie zgodności wykonania z dokumentacją projektową.

1.2.10.12. Trasy kablowe i okablowanie wewnętrzne

Generalny Wykonawca zobowiązany jest zaprojektować i wykonać trasy kablowe oraz okablowanie wewnętrzne serwerowni telekomunikacyjnej w sposób zapewniający separację instalacji, porządek eksploatacyjny, możliwość identyfikacji połączeń oraz bezpieczeństwo prac serwisowych.

Wymagania dotyczące tras kablowych obejmują co najmniej:

1) separację tras zasilających i sygnałowych;
2) separację okablowania miedzianego i światłowodowego, jeżeli zostanie zastosowane;
3) prowadzenie tras w sposób niekolidujący z istniejącymi kanałami sygnałowymi pomiędzy Serwerownią Główną a serwerownią telekomunikacyjną;
4) oznaczenie tras kablowych, przepustów, kabli i zakończeń;
5) zachowanie promieni gięcia, obciążeń mechanicznych i warunków montażowych wymaganych przez producentów kabli;
6) stosowanie przepustów i uszczelnień przeciwpożarowych w przejściach przez przegrody;
7) zapewnienie rezerwy miejsca na przyszłą rozbudowę;
8) wykonanie dokumentacji powykonawczej tras i połączeń.

Wszelkie nowe połączenia sygnałowe, zasilające, sterujące, alarmowe i monitorujące muszą zostać opisane, oznaczone i ujęte w dokumentacji powykonawczej. Generalny Wykonawca zobowiązany jest wykonać pomiary i testy zgodnie z wymaganiami właściwymi dla danej instalacji.

1.2.10.13. Kontrola dostępu

Elementy systemu kontroli dostępu do serwerowni telekomunikacyjnej muszą zostać włączone w istniejący w siedzibie Zamawiającego system kontroli dostępu oparty na rozwiązaniach firmy ROGER, zgodnie z dokumentacją powykonawczą modernizacji istniejącej instalacji kontroli dostępu oraz wymaganiami Zamawiającego.

Generalny Wykonawca zobowiązany jest zaprojektować, dostarczyć, zainstalować, skonfigurować, uruchomić i przetestować elementy kontroli dostępu w zakresie niezbędnym dla docelowego układu pomieszczenia po modernizacji.

System kontroli dostępu musi spełniać co najmniej następujące wymagania:

1) być kompatybilny z istniejącym systemem kontroli dostępu Zamawiającego;
2) umożliwiać zarządzanie dostępem z poziomu istniejącego narzędzia administracyjnego;
3) umożliwiać wykorzystanie istniejących mechanizmów nadawania uprawnień;
4) umożliwiać identyfikację osób uzyskujących dostęp do pomieszczenia;
5) umożliwiać rejestrację zdarzeń dostępu;
6) umożliwiać monitorowanie stanu kontrolera, czytników, drzwi i zdarzeń;

7) być objęty monitoringiem technicznym zgodnym z istniejącym modelem Zamawiającego;
8) zapewniać awaryjne otwarcie drzwi od strony wewnętrznej;
9) być wykonany z zachowaniem wymagań bezpieczeństwa fizycznego i przeciwpożarowego;
10) być udokumentowany w dokumentacji powykonawczej.

Generalny Wykonawca zobowiązany jest uwzględnić istniejące kontrolery, czytniki, magistrale komunikacyjne, adresację, segmentację sieciową, serwery zarządzające, bazę danych, aplikację administracyjną, monitoring oraz pliki konfiguracyjne istniejącego systemu. W przypadku konieczności rozbudowy istniejącego systemu Generalny Wykonawca dostarczy wszystkie wymagane komponenty, licencje, konfiguracje, prace instalacyjne i dokumentację.

1.2.10.14. System ochrony przeciwpożarowej i gaszenia

Serwerownia telekomunikacyjna musi zostać wyposażona albo dostosowana w zakresie zabezpieczeń przeciwpożarowych właściwych dla pomieszczeń technicznych i teleinformatycznych.

Generalny Wykonawca zobowiązany jest zaprojektować, dostarczyć, wykonać, uruchomić i przetestować rozwiązania ochrony przeciwpożarowej obejmujące co najmniej:

1) system detekcji pożaru właściwy dla pomieszczeń technicznych;
2) sygnalizację alarmową;
3) integrację z istniejącymi systemami bezpieczeństwa pożarowego budynku, jeżeli jest wymagana;
4) scenariusze współdziałania z zasilaniem, klimatyzacją, wentylacją, kontrolą dostępu i monitoringiem technicznym;
5) system gaszenia przeznaczony do pomieszczeń zawierających urządzenia teleinformatyczne;
6) oznakowanie, instrukcje i procedury eksploatacyjne;
7) testy, próby, odbiory i dokumentację powykonawczą.

Zastosowany system gaszenia musi być bezpieczny dla urządzeń teleinformatycznych, nie może powodować zniszczenia urządzeń elektronicznych podczas zadziałania, musi być zgodny z obowiązującymi przepisami i normami oraz musi zostać uzgodniony z Zamawiającym i właściwymi rzeczoznawcami, jeżeli takie uzgodnienia są wymagane.

1.2.10.15. Monitoring techniczny i zarządzanie infrastrukturą

Monitoring i zarządzanie infrastrukturą techniczną serwerowni telekomunikacyjnej muszą być tożsame albo w pełni kompatybilne z rozwiązaniami już istniejącymi u Zamawiającego lub z rozwiązaniami wdrażanymi przez Generalnego Wykonawcę w ramach niniejszego zamówienia.

Generalny Wykonawca zobowiązany jest objąć monitoringiem technicznym co najmniej:

1) temperaturę w pomieszczeniu i w przestrzeni pracy szaf RACK;
2) wilgotność, jeżeli funkcja taka zostanie przewidziana w projekcie;
3) stan zasilania podstawowego i gwarantowanego;
4) stan urządzeń zasilających i listew zasilających, jeżeli zostaną zastosowane;
5) stan systemu chłodzenia precyzyjnego;
6) stan drzwi i zdarzenia kontroli dostępu;
7) alarmy systemu przeciwpożarowego i gaszenia w zakresie możliwym do integracji;
8) stan urządzeń sieciowych, transmisyjnych i bezpieczeństwa zainstalowanych w pomieszczeniu;
9) stan szaf RACK i urządzeń pomocniczych, jeżeli zostaną wyposażone w odpowiednie czujniki;
10) zdarzenia krytyczne, ostrzegawcze i informacyjne.

System monitoringu musi umożliwiać prezentację alarmów, rejestrację zdarzeń, konfigurację progów alarmowych, przekazywanie powiadomień oraz integrację z centralnym modelem monitorowania zasobów RIS.

Generalny Wykonawca zobowiązany jest zapewnić, aby rozwiązania monitorowania były spójne z istniejącymi narzędziami Zamawiającego, w szczególności w zakresie sposobu prezentacji zdarzeń, nazewnictwa zasobów, progów alarmowych, raportowania, powiadamiania oraz dokumentowania konfiguracji.

1.2.10.16. Wymagania dotyczące urządzeń aktywnych i infrastruktury LAN

Serwerownia telekomunikacyjna pełni rolę węzła koncentracji dla segmentu sieci LAN. Generalny Wykonawca zobowiązany jest zaprojektować rozmieszczenie, zasilanie, okablowanie, chłodzenie i monitoring urządzeń aktywnych w taki sposób, aby zapewnić niezawodną pracę segmentu sieci LAN oraz jego powiązanie z Serwerownią Główną i infrastrukturą systemu RIS.

Jeżeli w ramach modernizacji serwerowni telekomunikacyjnej konieczne będzie czasowe przemieszczenie, przepięcie, rekonfiguracja albo wymiana urządzeń aktywnych, Generalny Wykonawca zobowiązany jest wykonać te czynności zgodnie z zaakceptowanym Planem Zachowania Ciągłości Działania Węzła Telekomunikacyjnego.

Wszelkie zmiany w konfiguracji urządzeń aktywnych, adresacji, VLAN, routingu, zabezpieczeniach, regułach dostępu, połączeniach międzyserwerownianych albo integracji

z istniejącą siecią Zamawiającego wymagają uprzedniej akceptacji Zamawiającego i muszą zostać ujęte w dokumentacji powykonawczej.

1.2.10.17. Wymagania dotyczące bezpieczeństwa i separacji

Modernizacja serwerowni telekomunikacyjnej musi zostać wykonana z zachowaniem wymagań cyberbezpieczeństwa, bezpieczeństwa fizycznego, bezpieczeństwa pożarowego, separacji instalacji oraz ciągłości działania.

Generalny Wykonawca zobowiązany jest zapewnić co najmniej:

1) separację torów zasilających od torów sygnałowych;
2) separację prac budowlanych od działających urządzeń teleinformatycznych;
3) zabezpieczenie urządzeń aktywnych przed pyłem, wilgocią, uszkodzeniami mechanicznymi i przypadkowym odłączeniem;
4) kontrolę dostępu do pomieszczenia podczas realizacji prac;
5) nadzór nad osobami wykonującymi prace w pomieszczeniu;
6) rejestrowanie zmian w konfiguracji urządzeń;
7) wykonywanie kopii konfiguracji przed zmianami;
8) możliwość przywrócenia stanu sprzed zmiany;
9) ochronę danych, konfiguracji, haseł, certyfikatów, kluczy i innych informacji wrażliwych;
10) zgodność z wymaganiami bezpieczeństwa określonymi w PFU i Umowie.

1.2.10.18. Testy, pomiary i odbiór

Generalny Wykonawca zobowiązany jest przeprowadzić testy, pomiary i odbiory wszystkich elementów modernizacji serwerowni telekomunikacyjnej.

Testy i odbiory muszą obejmować co najmniej:

1) odbiór prac budowlano-adaptacyjnych;
2) weryfikację likwidacji przejścia pomiędzy pokojem nr 32 a pokojem nr 31;
3) weryfikację docelowego układu jednego pomieszczenia technicznego;
4) odbiór podłogi technicznej albo jej dostosowania;
5) odbiór szaf RACK i ich wyposażenia;
6) test klimatyzacji pomieszczenia oraz systemu precyzyjnego chłodzenia szaf RACK;
7) test monitoringu temperatury, zasilania, klimatyzacji, drzwi i zdarzeń;
8) odbiór rozbudowy rozdzielnicy głównej w Serwerowni Głównej;
9) pomiary instalacji elektrycznej;
10) test toru zasilającego pomiędzy Serwerownią Główną a serwerownią telekomunikacyjną;
11) odbiór dedykowanego kanału kablowego dla toru zasilającego;
12) weryfikację braku negatywnego oddziaływania nowego kanału kablowego na istniejące okablowanie sygnałowe;

13) test systemu kontroli dostępu i jego integracji z istniejącym systemem Zamawiającego;
14) test systemów przeciwpożarowych i gaszenia;
15) testy urządzeń aktywnych i połączeń LAN objętych modernizacją;
16) test zachowania ciągłości działania usług komunikacyjnych systemu RIS;
17) testy odtworzeniowe po wykonanych zmianach konfiguracyjnych;
18) weryfikację oznaczeń kabli, urządzeń, szaf, tras, obwodów i zabezpieczeń;
19) weryfikację kompletności dokumentacji powykonawczej;
20) weryfikację przekazania instrukcji eksploatacyjnych i serwisowych.

Pozytywny wynik testów i odbiorów musi zostać potwierdzony protokołami podpisanymi przez Strony.

1.2.10.19. Dokumentacja powykonawcza i eksploatacyjna

Generalny Wykonawca zobowiązany jest przekazać Zamawiającemu kompletną dokumentację powykonawczą i eksploatacyjną modernizacji serwerowni telekomunikacyjnej.

Dokumentacja musi obejmować co najmniej:

1) opis wykonanych prac;
2) rzut pomieszczenia po modernizacji;
3) dokumentację zamurowania przejścia do pokoju nr 31;
4) schematy instalacji elektrycznej;
5) schemat rozbudowy rozdzielnicy głównej w Serwerowni Głównej;
6) schemat toru zasilającego i kanału kablowego pomiędzy serwerowniami;
7) dokumentację tras kablowych;
8) dokumentację okablowania sygnałowego, sterującego, monitorującego i zasilającego;
9) wykaz szaf RACK i ich wyposażenia;
10) dokumentację systemu chłodzenia precyzyjnego;
11) dokumentację kontroli dostępu;
12) dokumentację systemów przeciwpożarowych i gaszenia;
13) dokumentację monitoringu technicznego;
14) wyniki pomiarów elektrycznych;
15) wyniki pomiarów i testów okablowania;
16) protokoły testów i odbiorów;
17) wykaz urządzeń, numerów seryjnych, licencji, gwarancji i wsparcia producentów;
18) instrukcje eksploatacyjne;

19) instrukcje postępowania awaryjnego;

20) kopie konfiguracji urządzeń objętych modernizacją;

21) wykaz kont, uprawnień, dostępów i ról administracyjnych przekazanych Zamawiającemu;

22) zalecenia dotyczące przeglądów, konserwacji i dalszego utrzymania.

Dokumentacja musi zostać przekazana w formie elektronicznej edytowalnej, elektronicznej nieedytowalnej oraz papierowej, jeżeli wymagają tego postanowienia Umowy albo Zamawiający.

1.2.10.20. Rezultat końcowy

Rezultatem końcowym zadania musi być jedno, zmodernizowane, funkcjonalnie wydzielone, bezpieczne i gotowe do eksploatacji pomieszczenie serwerowni telekomunikacyjnej w pokoju nr 32, pełniące rolę węzła koncentracji sieci LAN oraz węzła telekomunikacyjnego systemu RIS.

Pomieszczenie musi być wyposażone w infrastrukturę zasilania, szafy RACK, klimatyzację pomieszczenia, system precyzyjnego chłodzenia szaf RACK, kontrolę dostępu, monitoring techniczny, zabezpieczenia przeciwpożarowe, system gaszenia, trasy kablowe, oznaczenia, dokumentację oraz wszystkie elementy niezbędne do stabilnej i bezpiecznej pracy urządzeń teleinformatycznych.

Modernizacja musi zostać wykonana bez nieuzgodnionego przerwania ciągłości komunikacji lokalizacji systemu informacji rzecznej z systemem centralnym oraz bez negatywnego wpływu na istniejące okablowanie sygnałowe pomiędzy Serwerownią Główną a serwerownią telekomunikacyjną.

1.2.11. Wymagania dla modernizacji sieci teleinformatycznej

1.2.11.1. Przedmiot zadania

Przedmiotem zadania jest zaprojektowanie, wykonanie, uruchomienie, przetestowanie i przekazanie do eksploatacji zmodernizowanej sieci teleinformatycznej w wybranych pomieszczeniach siedziby Zamawiającego zlokalizowanej w budynku tzw. Czerwonego Ratusza.

Modernizacja obejmuje wykonanie nowej instalacji teleinformatycznej oraz powiązanej infrastruktury punktów elektryczno-logicznych w zachodnim skrzydle budynku, w pomieszczeniach położonych na parterze, zgodnie z zakresem określonym w rozdziale 1.1.2.9. Modernizacja sieci teleinformatycznej.

Modernizowana sieć teleinformatyczna musi zostać wykonana jako uporządkowana instalacja okablowania strukturalnego kategorii 6, zapewniająca obsługę stanowisk pracy, urządzeń końcowych, urządzeń sieciowych, tabletów informacyjnych, urządzeń peryferyjnych oraz

pozostałych potrzeb Zamawiającego związanych z eksploatacją infrastruktury teleinformatycznej, systemów dziedzinowych i usług RIS.

1.2.11.2. Zakres lokalizacyjny

Modernizacja obejmuje następujące pomieszczenia zlokalizowane na parterze budynku:

- 19A;
- 20;
- 23A;
- 23B;
- 23C;
- 24;
- 25;
- 26;
- 27;
- 28;
- 29;
- 29A;
- 29B;
- 30.

Łącznie zakresem zadania objętych jest 15 pomieszczeń.

Generalny Wykonawca zobowiązany jest przed rozpoczęciem projektowania zweryfikować rzeczywisty układ pomieszczeń, przebieg istniejących instalacji, lokalizację istniejących punktów elektrycznych i logicznych, stan posadzek, ścian, sufitów, warunki prowadzenia tras kablowych, dostępność przestrzeni na poziomie -1 oraz powiązania z właściwymi punktami koncentracji sieci.

1.2.11.3. Zakres rzeczowy modernizacji

Zakres rzeczowy zadania obejmuje co najmniej:

1) wykonanie inwentaryzacji stanu istniejącego;
2) opracowanie dokumentacji projektowej modernizacji sieci teleinformatycznej;
3) zaprojektowanie przebiegu tras kablowych dla torów sygnałowych i zasilających;
4) wykonanie tras kablowych zgodnie z wymaganiami Zamawiającego;

5) wykonanie okablowania strukturalnego kategorii 6;
6) wykonanie punktów elektryczno-logicznych PEL;
7) wykonanie dodatkowych punktów logicznych RJ45 PoE przeznaczonych dla tabletów informacyjnych przy wejściach do pomieszczeń;
8) wykonanie podłogowego punktu PEL w sali konferencyjnej, tj. w pomieszczeniu 29B;
9) wykonanie zakończeń kablowych w pomieszczeniach oraz w punktach koncentracji;
10) dostawę, montaż, konfigurację i uruchomienie przełączników dostępowych PoE;
11) wykonanie połączeń przełączników dostępowych z właściwymi przełącznikami szkieletowymi Zamawiającego;
12) wykonanie oznaczeń gniazd, kabli, patch paneli, tras i urządzeń;
13) wykonanie pomiarów, testów i dokumentacji pomiarowej;
14) wykonanie dokumentacji powykonawczej;
15) odtworzenie powierzchni budowlanych naruszonych podczas prac;
16) przekazanie instalacji do eksploatacji.

1.2.11.4. Wymagania dotyczące dokumentacji projektowej

Generalny Wykonawca zobowiązany jest opracować dokumentację projektową modernizacji sieci teleinformatycznej i przedłożyć ją Zamawiającemu do akceptacji przed rozpoczęciem prac wykonawczych.

Dokumentacja projektowa musi obejmować co najmniej:

1) opis stanu istniejącego;
2) rzut pomieszczeń objętych modernizacją;
3) rozmieszczenie projektowanych punktów PEL;
4) rozmieszczenie projektowanych punktów RJ45 PoE dla tabletów informacyjnych;
5) rozmieszczenie podłogowego punktu PEL w pomieszczeniu 29B;
6) przebieg projektowanych tras kablowych na poziomie -1;
7) miejsca wykonania przewiertów pomiędzy kondygnacjami;
8) sposób wprowadzenia okablowania do poszczególnych pomieszczeń;
9) sposób prowadzenia tras kablowych w obrębie pomieszczeń;
10) przypisanie punktów logicznych do właściwych punktów koncentracji;
11) schemat połączeń logicznych i fizycznych;
12) sposób zasilania punktów PEL;
13) sposób separacji torów sygnałowych i zasilających;
14) sposób ochrony przeciwporażeniowej, przeciwprzepięciowej, uziemienia i połączeń wyrównawczych;

15) zestawienie materiałów, kabli, osprzętu, gniazd, patch paneli, przełączników, wkładek, kabli krosowych i akcesoriów;
16) opis technologii wykonania prac w budynku zabytkowym;
17) opis sposobu zabezpieczenia istniejących instalacji i pomieszczeń;
18) opis sposobu odtworzenia powierzchni po wykonanych pracach;
19) plan testów i pomiarów;
20) analizę ryzyk związanych z realizacją prac w działającym budynku.

Dokumentacja projektowa musi zostać opracowana z uwzględnieniem zabytkowego charakteru budynku, estetyki korytarzy, ograniczenia ingerencji w substancję budowlaną, konieczności zachowania bezpieczeństwa użytkowników budynku oraz ciągłości pracy Zamawiającego.

1.2.11.5. Zasady prowadzenia tras kablowych

Z uwagi na zabytkowy charakter budynku oraz konieczność zachowania estetyki korytarzy nie dopuszcza się prowadzenia tras kablowych po korytarzach budynku.

Zakaz, o którym mowa powyżej, obejmuje w szczególności prowadzenie po korytarzach:

1) natynkowych koryt kablowych;
2) listew instalacyjnych;
3) drabinek kablowych;
4) rur instalacyjnych;
5) peszli;
6) przewodów prowadzonych luzem;
7) elementów maskujących trasy kablowe;
8) innych widocznych elementów instalacji kablowej, które mogłyby naruszać estetykę korytarzy albo substancję zabytkową budynku.

Bazowym sposobem prowadzenia tras kablowych torów sygnałowych oraz zasilających jest wykorzystanie korytarza technicznego na poziomie -1 budynku. Wprowadzenie kabli do poszczególnych pomieszczeń na parterze musi być realizowane poprzez przewierty pomiędzy kondygnacjami prowadzone po skosie, w sposób umożliwiający wprowadzenie okablowania bezpośrednio do danego pomieszczenia.

Przewierty pomiędzy kondygnacjami muszą być projektowane i wykonywane w sposób:

1) ograniczający ingerencję w elementy konstrukcyjne budynku;
2) nienaruszający istniejących instalacji;

3) umożliwiający bezpieczne wprowadzenie okablowania do pomieszczenia;
4) zachowujący wymagane promienie gięcia kabli;
5) zapewniający możliwość wykonania uszczelnień przeciwpożarowych;
6) zapewniający możliwość późniejszej identyfikacji przebiegu trasy;
7) zgodny z wymaganiami BHP, ochrony przeciwpożarowej i przepisami budowlanymi;
8) zaakceptowany przez Zamawiającego przed wykonaniem.

Odstępstwa od zasady prowadzenia tras kablowych przez poziom -1 oraz od zasady wprowadzania kabli do pomieszczeń poprzez przewierty skośne wymagają każdorazowo uprzedniego uzgodnienia i akceptacji Zamawiającego. Generalny Wykonawca zobowiązany jest przedstawić uzasadnienie odstępstwa, proponowany przebieg alternatywny, analizę wpływu na estetykę budynku, bezpieczeństwo pożarowe, eksploatację, dostęp serwisowy oraz możliwość późniejszej rozbudowy.

1.2.11.6. Prowadzenie tras kablowych w pomieszczeniach

W obrębie pomieszczeń objętych modernizacją trasy kablowe należy prowadzić w sposób estetyczny, trwały, uporządkowany i możliwie niewidoczny dla użytkowników pomieszczeń.

Dopuszcza się następujące sposoby prowadzenia tras kablowych w pomieszczeniach:

1) podtynkowo;
2) pod posadzką;
3) w zagłębionych w posadzce systemowych korytach kablowych z pokrywami zlicowanymi z poziomem posadzki;
4) w innych rozwiązaniach uzgodnionych z Zamawiającym, jeżeli wynikają z uwarunkowań technicznych danego pomieszczenia i nie pogarszają estetyki, bezpieczeństwa ani funkcjonalności.

Nie dopuszcza się prowadzenia tras kablowych w sposób prowizoryczny, narażający przewody na uszkodzenia mechaniczne, utrudniający utrzymanie pomieszczeń, powodujący zagrożenie potknięcia, ograniczający funkcjonalność pomieszczeń albo niezgodny z charakterem zabytkowego budynku.

Po wykonaniu tras kablowych Generalny Wykonawca zobowiązany jest odtworzyć naruszone powierzchnie ścian, sufitów i posadzek. Odtworzenie musi zostać wykonane z należytą starannością, z zastosowaniem materiałów zgodnych z istniejącym wykończeniem albo materiałów zaakceptowanych przez Zamawiającego.

1.2.11.7. Separacja instalacji sygnałowych i zasilających

Generalny Wykonawca zobowiązany jest zapewnić separację torów sygnałowych i zasilających zgodnie z obowiązującymi normami, przepisami, zasadami wiedzy technicznej oraz wymaganiami producentów zastosowanego okablowania i osprzętu.

Separacja musi obejmować co najmniej:

1) właściwe odległości pomiędzy przewodami zasilającymi i sygnałowymi;
2) odrębne prowadzenie kabli w trasach, jeżeli wymagają tego przepisy, normy albo warunki techniczne;
3) stosowanie przegród separacyjnych w kanałach kablowych, jeżeli jest to wymagane;
4) unikanie równoległego prowadzenia torów zasilających i sygnałowych na krótkich odległościach bez wymaganej separacji;
5) właściwe wykonywanie skrzyżowań torów zasilających i sygnałowych;
6) ochronę przed zakłóceniami elektromagnetycznymi;
7) ochronę przed uszkodzeniem mechanicznym;
8) jednoznaczne oznaczenie torów i zakończeń.

Wymaganie separacji dotyczy zarówno tras prowadzonych na poziomie -1, przewiertów między kondygnacjami, jak i tras prowadzonych w obrębie pomieszczeń.

1.2.11.8. Punkty elektryczno-logiczne PEL

W każdym pomieszczeniu objętym modernizacją Generalny Wykonawca zobowiązany jest wykonać po dwa punkty elektryczno-logiczne PEL, z zastrzeżeniem wyjątków określonych w niniejszym rozdziale.

Każdy PEL musi obejmować co najmniej:

1) dwa gniazda zasilające w standardzie Schuko;
2) dwa punkty logiczne zakończone złączem RJ45;
3) ramki, puszki, osprzęt, oznaczenia i elementy montażowe niezbędne do prawidłowej eksploatacji;
4) powiązanie z właściwym punktem koncentracji sieci;
5) oznaczenie zgodne z dokumentacją powykonawczą.

Wyjątek od podstawowego założenia dwóch PEL w pomieszczeniu dotyczy pomieszczenia nr 30, w którym należy wykonać cztery punkty PEL.

W pomieszczeniu 29B, pełniącym funkcję sali konferencyjnej, należy dodatkowo wykonać podłogowy punkt PEL pod stołem konferencyjnym. Punkt ten musi zostać wykonany w sposób bezpieczny, estetyczny, trwały i umożliwiający użytkowanie sali konferencyjnej bez ryzyka uszkodzenia przewodów, potknięcia, zalania albo utrudnienia eksploatacji.

1.2.11.9. Punkty logiczne RJ45 PoE dla tabletów informacyjnych

W każdym pomieszczeniu objętym modernizacją Generalny Wykonawca zobowiązany jest wykonać dodatkowy punkt logiczny RJ45 przy drzwiach wejściowych do pomieszczenia, przeznaczony do komunikacji i zasilania tabletu informacyjnego w technologii PoE.

Punkt RJ45 PoE dla tabletu informacyjnego musi spełniać co najmniej następujące wymagania:

1) być zlokalizowany przy wejściu do pomieszczenia, w miejscu umożliwiającym montaż tabletu informacyjnego;
2) być zakończony złączem RJ45;
3) być wykonany w tej samej kategorii okablowania co pozostała instalacja logiczna;
4) być podłączony do przełącznika PoE;
5) umożliwiać zasilanie urządzenia końcowego w standardzie PoE właściwym dla przyjętego rozwiązania;
6) być oznaczony w sposób jednoznacznie odróżniający go od pozostałych punktów logicznych;
7) zostać ujęty w dokumentacji powykonawczej i wynikach pomiarów.

1.2.11.10. Minimalny zakres ilościowy punktów

Minimalny zakres ilościowy instalacji obejmuje co najmniej:

1) 33 punkty PEL;
2) 66 gniazd zasilających Schuko w punktach PEL;
3) 66 punktów logicznych RJ45 w punktach PEL;
4) 15 dodatkowych punktów logicznych RJ45 PoE dla tabletów informacyjnych;
5) łącznie co najmniej 81 punktów logicznych RJ45.

Powyższe wartości stanowią minimalny zakres ilościowy. Generalny Wykonawca zobowiązany jest zweryfikować kompletność zakresu na etapie inwentaryzacji i projektowania oraz uwzględnić wszystkie elementy konieczne do prawidłowego wykonania instalacji, nawet jeżeli nie zostały wprost wymienione w powyższym zestawieniu.

1.2.11.11. Okablowanie strukturalne

Modernizowana instalacja teleinformatyczna musi zostać wykonana jako okablowanie strukturalne kategorii 6 albo wyższej, jeżeli Generalny Wykonawca zaproponuje rozwiązanie korzystniejsze i zaakceptowane przez Zamawiającego.

Okablowanie strukturalne musi spełniać co najmniej następujące wymagania:

1) wszystkie elementy toru transmisyjnego muszą być zgodne z kategorią instalacji;
2) kable, gniazda, patch panele, złącza i pozostały osprzęt muszą pochodzić z jednego spójnego systemu okablowania albo być wzajemnie kompatybilne i objęte gwarancją producenta;
3) długości torów transmisyjnych muszą być zgodne z wymaganiami norm i producentów;
4) instalacja musi zostać zakończona w sposób umożliwiający administrację, pomiary, identyfikację i przyszłą rozbudowę;
5) każdy tor logiczny musi zostać jednoznacznie oznaczony po obu stronach;
6) każdy tor logiczny musi zostać objęty pomiarem certyfikacyjnym;
7) wyniki pomiarów muszą zostać przekazane Zamawiającemu w dokumentacji powykonawczej;
8) instalacja musi być wykonana przez osoby posiadające kwalifikacje i doświadczenie właściwe dla wykonywania okablowania strukturalnego.

Jeżeli producent systemu okablowania oferuje systemową gwarancję niezawodności, Generalny Wykonawca zobowiązany jest zapewnić możliwość objęcia wykonanej instalacji taką gwarancją, o ile jest to możliwe dla zastosowanego systemu i zakresu prac.

1.2.11.12. Punkty koncentracji sieci

Punktem koncentracji dla pomieszczeń 19A i 20 jest Serwerownia Główna.

Punktem koncentracji dla pozostałych pomieszczeń objętych modernizacją jest serwerownia pełniąca rolę węzła telekomunikacyjnego, modernizowana w ramach niniejszego zamówienia.

Generalny Wykonawca zobowiązany jest zaprojektować i wykonać zakończenia kablowe w punktach koncentracji w sposób uporządkowany, czytelny, opisany i umożliwiający późniejszą administrację. Zakończenia muszą zostać wykonane na patch panelach albo w innym rozwiązaniu właściwym dla przyjętej architektury, zaakceptowanym przez Zamawiającego.

Wszystkie połączenia do punktów koncentracji muszą zostać ujęte w dokumentacji powykonawczej wraz z numeracją, opisem, lokalizacją gniazda, numerem pomieszczenia, numerem patch panelu, numerem portu oraz wynikiem pomiaru.

1.2.11.13. Przełączniki dostępowe PoE

Generalny Wykonawca zobowiązany jest dostarczyć, zamontować, skonfigurować i uruchomić przełączniki dostępowe PoE niezbędne do obsługi punktów logicznych wykonywanych w ramach modernizacji.

Wymaga się dostawy co najmniej dwóch przełączników dostępowych PoE 48-portowych albo odpowiedniej wielokrotności przełączników PoE 24-portowych, zapewniającej wymaganą liczbę portów, rezerwę eksploatacyjną, możliwość obsługi punktów RJ45 PoE dla tabletów informacyjnych oraz możliwość dalszej rozbudowy.

Przełączniki dostępowe muszą spełniać co najmniej następujące wymagania:

1) obsługa PoE dla portów przeznaczonych do zasilania tabletów informacyjnych i innych urządzeń końcowych;
2) liczba portów umożliwiająca obsługę wszystkich punktów wykonanych w ramach modernizacji oraz zapewnienie rezerwy portów;
3) możliwość pracy zarządzalnej;
4) możliwość konfiguracji VLAN;
5) możliwość monitorowania stanu portów, zasilania PoE, obciążenia i zdarzeń;
6) możliwość integracji z istniejącą infrastrukturą sieciową Zamawiającego;
7) możliwość połączenia przełączników w stos albo zastosowania innego rozwiązania zapewniającego spójną administrację i niezawodną eksploatację;
8) możliwość podłączenia do istniejących przełączników szkieletowych Zamawiającego Dell S5224F-ON 24x 25GbE SFP albo do rozwiązania równoważnego wykorzystywanego przez Zamawiającego;
9) komplet wymaganych wkładek, kabli, modułów, kabli stakujących, uchwytów, zasilaczy, licencji, aktywacji funkcji i elementów montażowych;
10) objęcie gwarancją i wsparciem producenta przez okres wymagany w PFU i Umowie.

Wskazanie modelu Dell S5224F-ON dotyczy istniejącego zasobu Zamawiającego, do którego muszą zostać podłączone dostarczane przełączniki dostępowe. Generalny Wykonawca zobowiązany jest zapewnić kompatybilność dostarczanych urządzeń z istniejącą infrastrukturą Zamawiającego.

1.2.11.14. Zasilanie punktów PEL i urządzeń sieciowych

Generalny Wykonawca zobowiązany jest wykonać zasilanie punktów PEL oraz urządzeń sieciowych w sposób zgodny z obowiązującymi przepisami, normami, dokumentacją projektową i wymaganiami Zamawiającego.

Instalacja zasilająca musi spełniać co najmniej następujące wymagania:

1) zapewniać bezpieczne zasilanie wszystkich gniazd Schuko w punktach PEL;
2) zapewniać bezpieczne zasilanie urządzeń sieciowych w punktach koncentracji;
3) zapewniać właściwy dobór zabezpieczeń, przewodów, osprzętu i tras;
4) zapewniać ochronę przeciwporażeniową i przeciwprzepięciową;
5) zapewniać jednoznaczne oznaczenie obwodów;
6) zapewniać separację od torów sygnałowych;
7) być objęta pomiarami elektrycznymi;
8) zostać ujęta w dokumentacji powykonawczej.

Jeżeli zasilanie urządzeń aktywnych ma być realizowane z infrastruktury zasilania gwarantowanego albo zasilania serwerowni, Generalny Wykonawca zobowiązany jest uzgodnić to z Zamawiającym i wykazać w dokumentacji projektowej.

1.2.11.15. Wymagania dotyczące zabytkowego charakteru budynku i estetyki wykonania

Realizacja prac musi uwzględniać zabytkowy charakter budynku oraz wymóg zachowania estetyki korytarzy i pomieszczeń.

Generalny Wykonawca zobowiązany jest:

1) ograniczyć ingerencję w substancję budowlaną do minimum niezbędnego dla wykonania zadania;
2) nie prowadzić tras kablowych po korytarzach;
3) nie wykonywać widocznych elementów instalacji w korytarzach bez uprzedniej akceptacji Zamawiającego;
4) zabezpieczyć elementy wykończenia budynku przed uszkodzeniem;
5) prowadzić prace w sposób ograniczający zapylenie, hałas i uciążliwości dla użytkowników budynku;
6) odtworzyć naruszone powierzchnie w standardzie nie gorszym niż przed rozpoczęciem prac;
7) uzgodnić z Zamawiającym wygląd widocznych elementów osprzętu w pomieszczeniach;
8) stosować rozwiązania estetyczne, trwałe i dopasowane do charakteru pomieszczeń;
9) prowadzić dokumentację fotograficzną stanu przed rozpoczęciem prac i po ich zakończeniu.

1.2.11.16. Organizacja prac i minimalizacja uciążliwości

Generalny Wykonawca zobowiązany jest prowadzić prace w sposób minimalizujący wpływ na bieżące funkcjonowanie Zamawiającego.

Wymaga się co najmniej:

1) uzgodnienia harmonogramu prac z Zamawiającym;
2) uzgodnienia kolejności realizacji prac w pomieszczeniach;
3) wcześniejszego informowania Zamawiającego o pracach uciążliwych;
4) zabezpieczenia miejsc pracy;
5) zapewnienia bezpiecznego dostępu użytkowników do pomieszczeń, jeżeli pomieszczenia pozostają w użytkowaniu;
6) bieżącego usuwania odpadów, pyłu i zanieczyszczeń;
7) wykonywania prac powodujących największe uciążliwości w terminach uzgodnionych z Zamawiającym;
8) ochrony istniejących instalacji, mebli, urządzeń i wyposażenia;
9) przywrócenia pomieszczeń do stanu umożliwiającego użytkowanie po zakończeniu prac w danym obszarze.

1.2.11.17. Oznakowanie i administracja instalacją

Wszystkie elementy modernizowanej sieci teleinformatycznej muszą zostać oznakowane w sposób trwały, czytelny i zgodny z dokumentacją powykonawczą.

Oznakowaniu podlegają co najmniej:

1) punkty PEL;
2) punkty RJ45 PoE dla tabletów informacyjnych;
3) podłogowy punkt PEL w sali konferencyjnej;
4) kable logiczne;
5) kable zasilające;
6) patch panele;
7) porty przełączników;
8) trasy kablowe;
9) przepusty i przewierty;
10) szafy i elementy punktów koncentracji;
11) obwody elektryczne;
12) zabezpieczenia.

System oznaczeń musi umożliwiać jednoznaczne powiązanie gniazda w pomieszczeniu z zakończeniem w punkcie koncentracji i portem urządzenia aktywnego.

1.2.11.18. Testy, pomiary i odbiór

Generalny Wykonawca zobowiązany jest wykonać testy, pomiary i odbiory modernizowanej sieci teleinformatycznej.

Zakres testów i odbiorów musi obejmować co najmniej:

1) weryfikację zgodności wykonania z dokumentacją projektową;
2) weryfikację liczby i rozmieszczenia punktów PEL;
3) weryfikację liczby i rozmieszczenia punktów RJ45 PoE dla tabletów informacyjnych;
4) weryfikację wykonania podłogowego punktu PEL w pomieszczeniu 29B;
5) weryfikację zakazu prowadzenia tras kablowych po korytarzach;
6) weryfikację wykorzystania tras kablowych na poziomie -1;
7) weryfikację wykonania przewiertów skośnych do pomieszczeń;
8) weryfikację separacji torów sygnałowych i zasilających;
9) pomiary certyfikacyjne wszystkich torów logicznych;
10) pomiary instalacji elektrycznej;
11) test działania przełączników dostępowych PoE;
12) test zasilania urządzeń PoE;
13) test komunikacji pomiędzy punktami końcowymi a punktami koncentracji;
14) test połączenia przełączników dostępowych z przełącznikami szkieletowymi Zamawiającego;
15) weryfikację oznaczeń;
16) weryfikację zgodności dokumentacji powykonawczej ze stanem faktycznym;
17) weryfikację odtworzenia powierzchni po pracach instalacyjnych;
18) odbiór porządkowy i estetyczny pomieszczeń.

Pozytywny wynik testów i odbiorów musi zostać potwierdzony protokołami podpisanymi przez Strony.

1.2.11.19. Dokumentacja powykonawcza

Generalny Wykonawca zobowiązany jest przekazać Zamawiającemu kompletną dokumentację powykonawczą modernizacji sieci teleinformatycznej.

Dokumentacja powykonawcza musi obejmować co najmniej:

1) opis wykonanych prac;
2) rzuty pomieszczeń z naniesionymi punktami PEL i punktami RJ45 PoE;
3) rzuty tras kablowych na poziomie -1;
4) lokalizację przewiertów pomiędzy kondygnacjami;
5) sposób wprowadzenia okablowania do poszczególnych pomieszczeń;
6) schematy połączeń logicznych i fizycznych;
7) zestawienie wszystkich punktów logicznych;
8) zestawienie wszystkich punktów zasilających;
9) zestawienie kabli, patch paneli, portów, przełączników i punktów końcowych;
10) dokumentację oznaczeń;
11) wyniki pomiarów certyfikacyjnych okablowania strukturalnego;
12) wyniki pomiarów elektrycznych;
13) konfigurację przełączników dostępowych;
14) kopie konfiguracji urządzeń aktywnych;
15) wykaz dostarczonych urządzeń, licencji, modułów, wkładek, kabli i akcesoriów;
16) dokumentację gwarancyjną;
17) dokumentację fotograficzną stanu po wykonaniu prac;
18) instrukcje eksploatacyjne i administracyjne;
19) zalecenia dotyczące utrzymania i przyszłej rozbudowy instalacji.

Dokumentacja musi zostać przekazana w formie elektronicznej edytowalnej, elektronicznej nieedytowalnej oraz papierowej, jeżeli wymagają tego postanowienia Umowy albo Zamawiający.

1.2.11.20. Rezultat końcowy

Rezultatem końcowym zadania musi być kompletna, uporządkowana, oznakowana, przetestowana i gotowa do eksploatacji sieć teleinformatyczna kategorii 6 w pomieszczeniach objętych modernizacją.

Modernizacja musi zapewnić co najmniej:

1) wykonanie wymaganej liczby punktów PEL;
2) wykonanie wymaganej liczby punktów logicznych RJ45;
3) wykonanie punktów RJ45 PoE dla tabletów informacyjnych;
4) wykonanie podłogowego punktu PEL w pomieszczeniu 29B;
5) podłączenie instalacji do właściwych punktów koncentracji;
6) uruchomienie przełączników dostępowych PoE;

7) połączenie przełączników z infrastrukturą szkieletową Zamawiającego;
8) brak tras kablowych prowadzonych po korytarzach budynku;
9) wykorzystanie poziomu -1 jako bazowego poziomu prowadzenia tras kablowych;
10) wykonanie przewiertów skośnych do pomieszczeń;
11) zachowanie estetyki pomieszczeń i korytarzy;
12) odtworzenie powierzchni naruszonych podczas prac;
13) przekazanie kompletnej dokumentacji powykonawczej;
14) możliwość bezpiecznej administracji, diagnostyki, utrzymania i rozbudowy sieci w przyszłości.

1.2.12. Wymagania dla doposażenia serwerowni głównej

Rozdział określa wymagania Zamawiającego dotyczące doposażenia serwerowni głównej systemu RIS w zakresie niezbędnym do zapewnienia odpowiedniej wydajności, dostępności, skalowalności, bezpieczeństwa i możliwości dalszej rozbudowy środowiska teleinformatycznego wykorzystywanego do świadczenia usług RIS.

Doposażenie serwerowni głównej obejmuje rozbudowę wybranych komponentów istniejącej infrastruktury serwerowej, sieciowej, pamięci masowej oraz środowiska kopii zapasowych i odtwarzania danych. Zakres ten ma umożliwić obsługę nowych i modernizowanych usług systemu RIS, zwiększonego wolumenu danych, dodatkowych strumieni wideo, danych z urządzeń terenowych, danych hydrologicznych i meteorologicznych, danych AIS/VHF/DGNSS, usług cyfrowych oraz mechanizmów monitorowania i zarządzania systemem.

Wymagania określone w niniejszym rozdziale dotyczą w szczególności:

1) rozbudowy kart sieciowych w serwerach kasetowych Dell EMC PowerEdge MX740c pracujących w środowisku Dell EMC PowerEdge MX7000;
2) rozbudowy macierzy dyskowej Dell EMC PowerVault ME4024;
3) rozbudowy rozwiązania Dell EMC Avamar DP4400 / Integrated Data Protection Appliance / PowerProtect DP4400;
4) wykonania niezbędnych prac instalacyjnych, konfiguracyjnych, integracyjnych, testowych i dokumentacyjnych;
5) zapewnienia ciągłości działania środowiska produkcyjnego systemu RIS w trakcie realizacji prac;
6) zapewnienia wymaganej gwarancji, wsparcia producenta, aktualizacji, dokumentacji powykonawczej oraz przekazania rozwiązania do eksploatacji.

Doposażenie serwerowni głównej musi zostać wykonane z uwzględnieniem istniejącej architektury technicznej Zamawiającego, w szczególności środowiska serwerów kasetowych, macierzy dyskowej, rozwiązania kopii zapasowych, sieci Data Center, segmentacji ruchu, zasad

bezpieczeństwa, mechanizmów wysokiej dostępności oraz wymagań ciągłości działania systemu RIS.

Generalny Wykonawca zobowiązany jest przed rozpoczęciem prac zweryfikować stan istniejący środowiska, wersje oprogramowania, konfiguracje, kompatybilność sprzętową i licencyjną, dostępne zasoby, ograniczenia eksploatacyjne oraz wpływ planowanych prac na działanie systemu RIS. Wyniki weryfikacji muszą zostać uwzględnione w dokumentacji projektowej, harmonogramie prac, planie testów oraz procedurach wdrożenia i wycofania zmian.

Wszystkie prace w serwerowni głównej muszą być realizowane w sposób minimalizujący ryzyko przerwy w działaniu systemu RIS, utraty danych, degradacji parametrów pracy, utraty wsparcia producenta albo naruszenia spójności konfiguracji środowiska. Prace wymagające ingerencji w środowisko produkcyjne muszą być planowane, uzgadniane z Zamawiającym i wykonywane w zaakceptowanych oknach serwisowych, z zapewnieniem możliwości odtworzenia stanu sprzed zmiany.

Dostarczone komponenty, licencje, oprogramowanie, aktualizacje i usługi muszą być nowe, pełnowartościowe, zgodne z wymaganiami producentów środowiska Zamawiającego, objęte wymaganym wsparciem oraz kompatybilne z eksploatowanym rozwiązaniem. Niedopuszczalne jest zastosowanie komponentów powodujących utratę gwarancji, utratę wsparcia producenta, ograniczenie funkcjonalności, obniżenie poziomu bezpieczeństwa, brak możliwości aktualizacji albo pogorszenie parametrów dostępności i wydajności środowiska.

Szczegółowe wymagania dla poszczególnych zadań doposażenia serwerowni głównej określono w kolejnych podrozdziałach niniejszego rozdziału.

1.2.12.1. Wymagania dotyczące rozbudowy kart sieciowych w serwerach kasetowych Dell EMC PowerEdge MX740c

1.2.12.1.1. Przedmiot zadania

Generalny Wykonawca zrealizuje dostawę, instalację, konfigurację, uruchomienie i przetestowanie dodatkowych kart sieciowych CNA 2 × 25GbE dla wszystkich posiadanych przez Zamawiającego serwerów kasetowych Dell EMC PowerEdge MX740c pracujących w środowisku Dell EMC PowerEdge MX7000.

Celem zadania jest rozdzielenie funkcji transmisji danych DATA, obejmującej komunikację IP systemów i usług RIS, od funkcji dostępu do zasobów pamięci masowej SAN / storage, w szczególności w celu umożliwienia niezależnej konfiguracji parametrów sieci storage, w tym obsługi ramek jumbo frames oraz optymalizacji transmisji do macierzy dyskowej.

1.2.12.1.2. Stan istniejący środowiska

Zamawiający posiada środowisko serwerowe oparte o dwie niezależne obudowy kasetowe Dell EMC PowerEdge MX7000, pracujące w konfiguracji MCM — Multi-Chassis Management. Obudowy tworzą jedną logiczną domenę zarządzania i są wyposażone w moduły Dell EMC MX9116N, Dell EMC MX7116N oraz moduły zarządzające Dell EMC MX9002M.

W środowisku zainstalowanych jest łącznie 8 serwerów kasetowych Dell EMC PowerEdge MX740c, po 4 serwery w każdej obudowie MX7000. Dodatkowo Zamawiający posiada pojedynczy serwer zarządzający typu rack Dell EMC PowerEdge R640.

Warstwa sieciowa środowiska blade opiera się na przełącznikach fabric Dell EMC MX9116N oraz modułach rozszerzających Dell EMC MX7116N. Moduły MX9116N realizują funkcje przełączania, agregacji ruchu i uplinków do nadrzędnej infrastruktury Data Center, natomiast moduły MX7116N pełnią funkcję rozszerzenia fabric i przekazują połączenia z serwerów kasetowych do modułów MX9116N.

1.2.12.1.3. Zakres serwerów objętych modernizacją

Generalny Wykonawca zrealizuje modernizację wszystkich 8 serwerów Dell EMC PowerEdge MX740c o następujących numerach seryjnych:

Tabela 5: Numery seryjne serwerów Dell EMC PowerEdge MX740c

Lp.	Typ serwera	Numer seryjny
1.	Dell EMC PowerEdge MX740c	3R8T7B3
2.	Dell EMC PowerEdge MX740c	4R8T7B3
3.	Dell EMC PowerEdge MX740c	5R8T7B3
4.	Dell EMC PowerEdge MX740c	6R8T7B3
5.	Dell EMC PowerEdge MX740c	DQ8T7B3
6.	Dell EMC PowerEdge MX740c	FQ8T7B3
7.	Dell EMC PowerEdge MX740c	GQ8T7B3
8.	Dell EMC PowerEdge MX740c	HQ8T7B3

1.2.12.1.4. Wymagania dotyczące dostarczanych kart sieciowych

Generalny Wykonawca dostarczy dla każdego serwera kasetowego jedną kartę sieciową QLogic 2x25GE QL41262HMKR CNA albo rozwiązanie równoważne.

Za rozwiązanie równoważne Zamawiający uzna kartę, która spełnia łącznie co najmniej następujące wymagania:

1) jest kompatybilna sprzętowo, mechanicznie, elektrycznie i programowo z serwerami Dell EMC PowerEdge MX740c;

2) jest przeznaczona do pracy w środowisku Dell EMC PowerEdge MX7000;
3) zapewnia minimum 2 porty Ethernet 25GbE;
4) obsługuje funkcje CNA — Converged Network Adapter — umożliwiające wykorzystanie karty do transmisji danych IP oraz ruchu storage;
5) obsługuje konfigurację ramek jumbo frames co najmniej do wartości MTU wymaganej przez środowisko storage Zamawiającego;
6) obsługuje mechanizmy VLAN, priorytetyzacji ruchu, agregacji i redundancji wymagane przez środowisko serwerowe;
7) posiada sterowniki i firmware wspierane dla systemów operacyjnych oraz platform wirtualizacyjnych eksploatowanych przez Zamawiającego;
8) jest widoczna i zarządzalna z poziomu narzędzi administracyjnych Dell właściwych dla środowiska PowerEdge MX;
9) posiada status rozwiązania wspieranego przez producenta serwerów albo producenta karty dla pracy w serwerach Dell EMC PowerEdge MX740c;
10) nie powoduje utraty gwarancji, wsparcia serwisowego ani możliwości aktualizacji firmware dla serwerów MX740c i środowiska MX7000.

Generalny Wykonawca przed dostawą przedstawi Zamawiającemu dokumentację potwierdzającą kompatybilność oferowanych kart z serwerami Dell EMC PowerEdge MX740c oraz środowiskiem PowerEdge MX7000.

1.2.12.1.5. Wymagania instalacyjne

Generalny Wykonawca wykona instalację kart sieciowych w serwerach kasetowych w sposób zgodny z dokumentacją producenta Dell EMC, zasadami obsadzenia modułów I/O w środowisku PowerEdge MX oraz aktualną konfiguracją dwóch obudów MX7000 pracujących w grupie MCM.

Generalny Wykonawca musi przed rozpoczęciem prac wykonać inwentaryzację techniczną środowiska, obejmującą co najmniej:

1) aktualne obsadzenie slotów w serwerach MX740c;
2) aktualną konfigurację fabric w obudowach MX7000;
3) konfigurację przełączników Dell EMC MX9116N;
4) konfigurację modułów Dell EMC MX7116N;
5) aktualną wersję firmware serwerów, kart, modułów fabric i modułów zarządzających;
6) dostępność portów i zasobów niezbędnych do uruchomienia dodatkowych interfejsów 25GbE;
7) konfigurację uplinków do nadrzędnej infrastruktury Data Center;
8) aktualny podział ruchu DATA, MGMT, storage i innych sieci wykorzystywanych przez system RIS.

Prace instalacyjne muszą zostać wykonane w uzgodnionym z Zamawiającym oknie serwisowym. Generalny Wykonawca musi opracować i uzgodnić z Zamawiającym plan prac, plan wyłączeń, plan odtworzenia konfiguracji oraz procedurę powrotu do stanu sprzed zmian.

1.2.12.1.6. Wymagania konfiguracyjne

Generalny Wykonawca skonfiguruje nowe karty sieciowe w sposób zapewniający logiczne i funkcjonalne rozdzielenie ruchu DATA od ruchu SAN / storage.

Konfiguracja musi obejmować co najmniej:

1) przypisanie nowych interfejsów 25GbE do właściwych profili serwerowych lub szablonów konfiguracji w środowisku PowerEdge MX;
2) konfigurację połączeń pomiędzy serwerami MX740c a warstwą fabric MX9116N / MX7116N;
3) konfigurację VLAN, trunków, sieci logicznych lub równoważnych mechanizmów separacji ruchu;
4) konfigurację ścieżek transmisyjnych dla ruchu storage;
5) konfigurację ramek jumbo frames dla sieci storage, zgodnie z wymaganiami macierzy dyskowej i hostów;
6) konfigurację redundancji połączeń, tak aby awaria pojedynczego portu, ścieżki, modułu fabric lub elementu uplink nie powodowała utraty dostępu do zasobów krytycznych;
7) konfigurację zgodną z aktualnym modelem wysokiej dostępności środowiska serwerowego;
8) aktualizację lub dostosowanie konfiguracji systemów operacyjnych, hypervisorów, przełączników wirtualnych, multipathingu i dostępu do macierzy dyskowej, jeżeli jest to wymagane dla pełnego uruchomienia nowych kart;
9) weryfikację zgodności parametrów MTU na całej ścieżce transmisyjnej pomiędzy serwerami a macierzą dyskową;
10) weryfikację braku negatywnego wpływu zmian na istniejące usługi RIS.

1.2.12.1.7. Wymagania dotyczące wysokiej dostępności

Generalny Wykonawca musi zachować albo podnieść dotychczasowy poziom wysokiej dostępności środowiska serwerowego. Rozbudowa nie może powodować powstania pojedynczego punktu awarii dla komunikacji DATA, zarządzania ani dostępu do zasobów storage.

Docelowa konfiguracja musi zapewniać co najmniej:

1) redundantne ścieżki transmisyjne z każdego serwera kasetowego do warstwy fabric;

2) redundantne połączenia do zasobów pamięci masowej;
3) możliwość pracy środowiska po awarii pojedynczego portu karty, pojedynczego modułu fabric albo pojedynczej ścieżki uplink;
4) spójność konfiguracji w obu obudowach MX7000;
5) zgodność konfiguracji z mechanizmami MCM środowiska PowerEdge MX;
6) brak asymetrii konfiguracyjnej pomiędzy serwerami, chyba że wynika ona z zatwierdzonej przez Zamawiającego architektury docelowej.

1.2.12.1.8. Wymagania dotyczące testów i odbioru

Generalny Wykonawca przeprowadzi testy instalacyjne, konfiguracyjne, funkcjonalne i wydajnościowe. Testy muszą potwierdzić poprawność instalacji kart, separację ruchu DATA i SAN / storage oraz poprawne działanie jumbo frames.

Minimalny zakres testów obejmuje:

1) potwierdzenie wykrywania kart przez serwery MX740c;
2) potwierdzenie poprawnego rozpoznania kart w narzędziach zarządzających Dell;
3) potwierdzenie zgodności wersji firmware i sterowników;
4) test dostępności obu portów 25GbE na każdej karcie;
5) test połączenia każdego serwera z właściwymi modułami fabric;
6) test poprawności konfiguracji VLAN i separacji ruchu;
7) test transmisji DATA po dotychczasowej albo docelowej ścieżce;
8) test transmisji storage po nowych interfejsach;
9) test MTU / jumbo frames na całej ścieżce serwer — fabric — sieć — macierz;
10) test multipathingu albo równoważnego mechanizmu redundancji dostępu do storage;
11) test przełączenia po awarii jednego portu;
12) test przełączenia po awarii jednej ścieżki transmisyjnej;
13) test wpływu zmian na uruchomione usługi systemu RIS;
14) test ponownego uruchomienia wybranego serwera i poprawnego odtworzenia konfiguracji;
15) test monitorowania i alarmowania dla nowych interfejsów.

Warunkiem odbioru jest uzyskanie pozytywnych wyników testów dla wszystkich 8 serwerów MX740c oraz przekazanie Zamawiającemu kompletnej dokumentacji powykonawczej.

1.2.12.1.9. Wymagania dotyczące dokumentacji

Generalny Wykonawca przekaże dokumentację powykonawczą obejmującą co najmniej:

1) wykaz dostarczonych kart z numerami seryjnymi;
2) przypisanie kart do konkretnych serwerów MX740c;
3) potwierdzenie kompatybilności zastosowanych kart;
4) opis wykonanych prac instalacyjnych;
5) schemat logiczny połączeń DATA i SAN / storage po rozbudowie;
6) opis konfiguracji portów, VLAN, MTU, redundancji i uplinków;
7) wykaz wersji firmware i sterowników;
8) kopię konfiguracji istotnych elementów środowiska przed zmianą i po zmianie;
9) procedurę administracyjną utrzymania nowych kart i interfejsów;
10) procedurę diagnostyczną dla awarii portu, karty, ścieżki fabric i dostępu do storage;
11) protokoły z przeprowadzonych testów;
12) rekomendacje dotyczące dalszej eksploatacji, aktualizacji firmware i monitorowania.

Dokumentacja musi zostać przekazana w wersji edytowalnej oraz PDF. Nazewnictwo elementów dokumentacji musi być spójne z aktualną dokumentacją eksploatacyjną środowiska RIS.

1.2.12.1.10. Wymagania dotyczące gwarancji i wsparcia

Generalny Wykonawca zapewni gwarancję i wsparcie serwisowe dla dostarczonych kart sieciowych oraz wykonanych prac instalacyjno-konfiguracyjnych.

Wymagania minimalne:

1) okres gwarancji nie krótszy niż okres gwarancji wymagany dla przedmiotu zamówienia;
2) wsparcie producenta albo autoryzowanego kanału serwisowego dla dostarczonych kart;
3) dostęp do aktualizacji firmware i sterowników przez cały okres gwarancji;
4) usunięcie błędów konfiguracyjnych ujawnionych po odbiorze w ramach gwarancji;
5) brak ograniczenia istniejącego wsparcia serwisowego dla serwerów Dell EMC PowerEdge MX740c, obudów MX7000, modułów MX9116N, MX7116N i MX9002M.

1.2.12.1.11. Wymagania dotyczące realizacji prac w środowisku produkcyjnym

Generalny Wykonawca musi prowadzić prace w sposób minimalizujący wpływ na ciągłość działania usług RIS. Każda czynność wymagająca przerwy w działaniu serwera, restartu, zmiany

konfiguracji fabric, zmiany profilu serwerowego albo zmiany konfiguracji sieciowej musi zostać wcześniej uzgodniona z Zamawiającym.

Generalny Wykonawca musi zapewnić:

1) wykonanie kopii konfiguracji przed rozpoczęciem zmian;
2) możliwość odtworzenia konfiguracji sprzed modernizacji;
3) prowadzenie dziennika prac;
4) udział osób posiadających doświadczenie w administracji środowiskami Dell EMC PowerEdge MX;
5) zachowanie zasad bezpieczeństwa dla infrastruktury krytycznej systemu RIS;
6) brak nieuzgodnionych zmian w konfiguracji produkcyjnej;
7) przekazanie Zamawiającemu informacji o wszystkich zmianach wykonanych w środowisku.

1.2.12.1.12. Rezultat końcowy

Rezultatem zadania musi być kompletna, uruchomiona i przetestowana rozbudowa sieciowa wszystkich 8 serwerów Dell EMC PowerEdge MX740c o dodatkowe interfejsy 2 × 25GbE CNA, umożliwiająca separację ruchu DATA od ruchu SAN / storage oraz wykorzystanie parametrów transmisyjnych wymaganych dla wydajnego dostępu do zasobów macierzy dyskowej, w tym jumbo frames.

Modernizacja musi zostać wykonana bez obniżenia poziomu dostępności środowiska serwerowego, bez utraty kompatybilności z istniejącą architekturą Dell EMC PowerEdge MX7000 i bez negatywnego wpływu na działanie usług systemu RIS.

1.2.12.2. Wymagania dotyczące rozbudowy macierzy dyskowej Dell EMC PowerVault ME4024

1.2.12.2.1. Przedmiot zadania

Generalny Wykonawca zrealizuje dostawę, instalację, konfigurację, uruchomienie i przetestowanie rozbudowy posiadanej przez Zamawiającego macierzy dyskowej Dell EMC PowerVault ME4024 o dodatkową półkę dyskową SSD.

Rozbudowa musi zwiększyć pojemność przestrzeni dyskowej udostępnianej hostom VMware vSphere za pomocą protokołu blokowego iSCSI, przy zachowaniu kompatybilności z istniejącą architekturą środowiska RIS, aktualną konfiguracją macierzy, zasadami wysokiej dostępności oraz dotychczasowym modelem wykorzystania przestrzeni jako datastore dla środowiska wirtualizacyjnego.

1.2.12.2.2. Stan istniejący

Zamawiający eksploatuje środowisko, w którym główne Datacenter DC-01 obejmuje 8 serwerów kasetowych korzystających ze współdzielonych zasobów dyskowych udostępnionych z macierzy Dell EMC PowerVault ME4024 za pomocą protokołu iSCSI.

Drugie Datacenter DC-02 obejmuje pojedynczy serwer fizyczny pełniący funkcję dedykowanego serwera zarządzającego. Serwer ten wykorzystuje lokalne dyski wewnętrzne dla maszyn wirtualnych uruchomionych na tym hoście, ale posiada również dostęp do zasobów współdzielonych udostępnionych z macierzy Dell EMC PowerVault ME4024 za pomocą iSCSI.

Obecna macierz Dell EMC PowerVault ME4024 jest wyposażona w 24 dyski SSD SAS 12 Gb/s o pojemności 3,84 TB każdy. Cała dostępna pojemność została zaaranżowana jako dwie grupy dyskowe po 12 dysków w trybie RAID ADAPT, o pojemności użytkowej 27,94 TB każda. Na macierzy utworzono dwa wolumeny: DataStore1 i DataStore2, udostępnione hostom VMware vSphere.

1.2.12.2.3. Wymagany zakres dostawy

Generalny Wykonawca dostarczy co najmniej:

1) jedną półkę rozszerzeń Dell EMC PowerVault ME424 albo rozwiązanie równoważne, w pełni kompatybilne z Dell EMC PowerVault ME4024;
2) 14 (12 + 2 hot spare) dysków SSD SAS 12 Gb/s, 2,5”, o pojemności nie mniejszej niż 3,84 TB każdy;
3) komplet szyn montażowych, elementów instalacyjnych i przewodów zasilających;
4) komplet przewodów SAS 12 Gb/s wymaganych do redundantnego podłączenia półki rozszerzeń do kontrolerów macierzy ME4024;
5) licencje, firmware, sterowniki, elementy aktywacyjne albo inne komponenty wymagane do prawidłowej pracy rozbudowanej macierzy, o ile są wymagane przez producenta;
6) dokumentację producenta potwierdzającą zgodność oferowanej półki i dysków z posiadaną macierzą Dell EMC PowerVault ME4024.

1.2.12.2.4. Wymagania dla półki dyskowej

Dostarczona półka dyskowa musi spełniać co najmniej następujące wymagania:

1) musi być półką rozszerzeń wspieraną przez producenta dla macierzy Dell EMC PowerVault ME4024;
2) musi zapewniać minimum 24 zatoki na dyski 2,5”;
3) musi obsługiwać dyski SSD SAS 12 Gb/s;
4) musi posiadać redundantne moduły rozszerzeń / IOM;

5) musi posiadać redundantne zasilacze i wentylatory zgodne z architekturą PowerVault ME4;
6) musi umożliwiać redundantne połączenie z kontrolerami macierzy bazowej;
7) musi być przeznaczona do montażu w szafie rack 19”;
8) musi być objęta wsparciem producenta dla pracy z Dell EMC PowerVault ME4024;
9) nie może powodować utraty gwarancji, wsparcia producenta ani możliwości aktualizacji firmware posiadanej macierzy;
10) musi zostać dostarczona jako komplet gotowy do instalacji, wraz ze wszystkimi elementami mechanicznymi, kablowymi i zasilającymi.

1.2.12.2.5. Wymagania dla dysków SSD

Generalny Wykonawca dostarczy dyski SSD spełniające co najmniej następujące wymagania:

1) typ: SSD;
2) format: 2,5”;
3) interfejs: SAS 12 Gb/s;
4) pojemność pojedynczego dysku: minimum 3,84 TB;
5) liczba dysków: 14 sztuk;
6) dyski muszą znajdować się na aktualnej liście wsparcia Dell dla Dell EMC PowerVault ME4 albo posiadać pisemne potwierdzenie Dell o zgodności z posiadaną macierzą ME4024;
7) dyski muszą być dostarczone w oryginalnych kieszeniach / carrierach zgodnych z PowerVault ME424;
8) dyski muszą posiadać firmware wymagany albo rekomendowany przez Dell dla pracy w macierzach ME4;
9) dyski nie mogą być dyskami wcześniej używanymi w macierzach ME5 albo innych systemach, jeżeli mogłoby to skutkować niezgodnością metadanych lub brakiem wsparcia producenta;
10) wszystkie dyski w ramach nowej grupy dyskowej muszą być jednorodne pod względem pojemności, typu, interfejsu i klasy wydajnościowej.

Zamawiający nie dopuszcza zastosowania dysków SSD o pojemności 7,68 TB albo 15,36 TB, chyba że Generalny Wykonawca przed dostawą przedstawi jednoznaczne potwierdzenie producenta Dell, że konkretny numer części, model dysku, firmware i konfiguracja są wspierane dla Dell EMC PowerVault ME4024.

1.2.12.2.6. Wymagania dotyczące konfiguracji pojemności

Generalny Wykonawca zaprojektuje i uzgodni z Zamawiającym docelowy sposób włączenia nowej pojemności do istniejącej macierzy.

Konfiguracja musi zostać wykonana w sposób zapewniający:

1) zachowanie istniejących wolumenów DataStore1 i DataStore2 bez utraty danych;
2) zachowanie dostępności istniejących datastore’ów dla hostów VMware vSphere;
3) utworzenie nowych grup dyskowych albo rozszerzenie istniejącej struktury wyłącznie w sposób wspierany przez producenta;
4) zastosowanie RAID ADAPT albo innego mechanizmu zabezpieczenia danych zatwierdzonego przez Zamawiającego;
5) zapewnienie przestrzeni rezerwowej / spare capacity zgodnie z zaleceniami Dell;
6) możliwość udostępnienia dodatkowej przestrzeni hostom VMware vSphere przez iSCSI;
7) zachowanie separacji i redundancji ścieżek dostępu do wolumenów;
8) brak obniżenia poziomu dostępności obecnie działających usług RIS.

Preferowanym wariantem konfiguracyjnym jest utworzenie na nowej półce dwóch analogicznych grup dyskowych po 12 dysków SSD 3,84 TB w RAID ADAPT oraz utworzenie nowych wolumenów przeznaczonych do wykorzystania jako dodatkowe datastore’y VMware, np. DataStore3 i DataStore4. Ostateczne nazwy wolumenów muszą zostać uzgodnione z Zamawiającym.

1.2.12.2.7. Wymagania dotyczące integracji z VMware vSphere

Generalny Wykonawca wykona pełną integrację nowej przestrzeni dyskowej ze środowiskiem VMware vSphere.

Zakres prac musi obejmować co najmniej:

1) utworzenie albo rozszerzenie wolumenów na macierzy;
2) przypisanie wolumenów do właściwych hostów VMware;
3) konfigurację mapowania hostów i inicjatorów iSCSI;
4) weryfikację poprawności widoczności LUN przez wszystkie uprawnione hosty;
5) konfigurację albo weryfikację multipathingu;
6) utworzenie datastore’ów VMware albo rozszerzenie istniejących datastore’ów — zgodnie z uzgodnioną koncepcją;
7) weryfikację poprawnej pracy datastore’ów w vCenter;
8) wykonanie testu migracji wybranej maszyny wirtualnej albo testowego pliku VM na nową przestrzeń;
9) weryfikację braku wpływu rozbudowy na działanie istniejących maszyn wirtualnych RIS.

1.2.12.2.8. Wymagania dotyczące iSCSI i sieci storage

Generalny Wykonawca musi zapewnić, że rozbudowa macierzy zostanie zintegrowana z istniejącą siecią iSCSI bez pogorszenia parametrów pracy środowiska.

Generalny Wykonawca musi zweryfikować i udokumentować co najmniej:

1) konfigurację portów iSCSI macierzy;
2) konfigurację inicjatorów iSCSI na hostach VMware;
3) konfigurację VLAN dla sieci storage;
4) konfigurację MTU, w tym jumbo frames, jeżeli są stosowane albo zostaną wdrożone w ramach odrębnego zadania;
5) konfigurację multipathingu;
6) redundancję ścieżek pomiędzy hostami a macierzą;
7) wpływ nowej pojemności na wydajność i obciążenie kontrolerów macierzy;
8) zgodność konfiguracji z dobrymi praktykami Dell oraz VMware dla iSCSI.

1.2.12.2.9. Wymagania instalacyjne

Generalny Wykonawca przed rozpoczęciem prac wykona inwentaryzację techniczną środowiska obejmującą co najmniej:

1) model, numer seryjny i konfigurację posiadanej macierzy Dell EMC PowerVault ME4024;
2) liczbę i typ kontrolerów;
3) wersję firmware kontrolerów, modułów I/O i dysków;
4) aktualną konfigurację grup dyskowych;
5) aktualną konfigurację wolumenów;
6) aktualne mapowania hostów i LUN;
7) konfigurację iSCSI;
8) konfigurację VMware vSphere w zakresie datastore’ów;
9) dostępność miejsca, zasilania i chłodzenia w szafie rack;
10) możliwość bezpiecznego wpięcia półki rozszerzeń do istniejącej macierzy.

Prace muszą zostać wykonane w uzgodnionym z Zamawiającym oknie serwisowym. Generalny Wykonawca musi opracować i przedstawić Zamawiającemu plan prac, plan testów, plan wyłączeń oraz procedurę wycofania zmian.

1.2.12.2.10. Wymagania dotyczące bezpieczeństwa danych

Generalny Wykonawca musi prowadzić prace w sposób eliminujący ryzyko utraty danych.

Przed rozpoczęciem prac Generalny Wykonawca musi:

1) zweryfikować stan macierzy i brak aktywnych alarmów krytycznych;
2) wykonać eksport konfiguracji macierzy;
3) potwierdzić z Zamawiającym stan kopii zapasowych maszyn wirtualnych;
4) przygotować procedurę odtworzenia konfiguracji w przypadku niepowodzenia prac;
5) potwierdzić poprawność działania istniejących wolumenów i datastore’ów;
6) potwierdzić, że rozbudowa nie wymaga operacji destrukcyjnych na istniejących grupach dyskowych.

Generalny Wykonawca nie może wykonywać operacji skutkujących usunięciem, inicjalizacją, nadpisaniem albo utratą dostępności istniejących danych bez odrębnej pisemnej zgody Zamawiającego.

1.2.12.2.11. Wymagania dotyczące testów odbiorowych

Generalny Wykonawca przeprowadzi testy odbiorowe obejmujące co najmniej:

1) weryfikację poprawności fizycznej instalacji półki;
2) weryfikację widoczności półki ME424 w narzędziach zarządzających macierzą;
3) weryfikację widoczności wszystkich 24 dysków SSD;
4) weryfikację poprawności firmware półki, modułów I/O i dysków;
5) weryfikację braku alarmów krytycznych i ostrzeżeń po instalacji;
6) test redundancji połączeń SAS między macierzą a półką;
7) test pracy po symulowanej utracie jednej ścieżki;
8) test utworzenia grup dyskowych;
9) test utworzenia wolumenów;
10) test mapowania wolumenów do hostów VMware;
11) test widoczności LUN na wszystkich uprawnionych hostach;
12) test multipathingu;
13) test utworzenia datastore’ów VMware;
14) test zapisu i odczytu danych na nowym datastore;
15) test migracji albo składowania testowej maszyny wirtualnej;
16) test monitorowania stanu macierzy po rozbudowie;

17) test zachowania dostępności istniejących datastore’ów DataStore1 i DataStore2.

Warunkiem odbioru jest bezbłędna praca nowej półki, widoczność pełnej dostarczonej pojemności zgodnie z zatwierdzoną konfiguracją, poprawne udostępnienie przestrzeni dla VMware oraz brak negatywnego wpływu na dotychczas działające usługi systemu RIS.

1.2.12.2.12. Wymagania dotyczące dokumentacji powykonawczej

Generalny Wykonawca przekaże dokumentację powykonawczą obejmującą co najmniej:

1) opis stanu przed rozbudową;
2) opis wykonanej rozbudowy;
3) wykaz dostarczonych urządzeń, dysków i kabli wraz z numerami seryjnymi;
4) potwierdzenie zgodności dostarczonych komponentów z Dell EMC PowerVault ME4024;
5) schemat połączeń SAS między macierzą bazową a półką rozszerzeń;
6) schemat logiczny grup dyskowych, wolumenów i datastore’ów;
7) konfigurację RAID ADAPT albo innego zastosowanego poziomu zabezpieczenia danych;
8) konfigurację host mapping / LUN mapping;
9) konfigurację iSCSI;
10) konfigurację multipathingu;
11) wykaz wersji firmware;
12) wyniki testów odbiorowych;
13) procedurę administracyjną dla nowych zasobów;
14) procedurę diagnostyczną dla awarii dysku, półki, ścieżki SAS, kontrolera i wolumenu;
15) zalecenia eksploatacyjne dotyczące monitorowania, aktualizacji firmware i wymiany dysków.

Dokumentacja musi zostać przekazana w wersji edytowalnej oraz PDF.

1.2.12.2.13. Wymagania dotyczące gwarancji i wsparcia

Generalny Wykonawca zapewni gwarancję i wsparcie serwisowe dla dostarczonej półki, dysków, okablowania oraz wykonanych prac instalacyjno-konfiguracyjnych.

Wymagania minimalne:

1) gwarancja nie krótsza niż okres gwarancji wymagany dla przedmiotu zamówienia;
2) wsparcie producenta Dell albo autoryzowanego partnera Dell;

3) dostęp do aktualizacji firmware dla półki, dysków i elementów macierzy;
4) usuwanie błędów konfiguracyjnych ujawnionych po odbiorze;
5) brak ograniczenia wsparcia dla istniejącej macierzy Dell EMC PowerVault ME4024;
6) wymiana uszkodzonych dysków i komponentów zgodnie z poziomem SLA wymaganym dla infrastruktury krytycznej systemu RIS.

1.2.12.2.14. Rezultat końcowy

Rezultatem zadania musi być rozbudowana, uruchomiona i przetestowana macierz Dell EMC PowerVault ME4024 z dodatkową półką SSD, zapewniająca zwiększoną pojemność przestrzeni dyskowej dla środowiska VMware vSphere wykorzystywanego przez system RIS.

Rozbudowa musi zostać wykonana bez utraty danych, bez obniżenia dostępności obecnych zasobów DataStore1 i DataStore2, bez utraty wsparcia producenta Dell oraz z zachowaniem pełnej zgodności z architekturą iSCSI, VMware vSphere i zasadami wysokiej dostępności infrastruktury Zamawiającego.

1.2.12.3. Wymagania dotyczące rozbudowy rozwiązania Dell EMC Avamar DP4400 / Integrated Data Protection Appliance / PowerProtect DP4400

1.2.12.3.1. Przedmiot zadania

Generalny Wykonawca zrealizuje dostawę, aktywację, konfigurację, uruchomienie i przetestowanie rozbudowy posiadanego przez Zamawiającego rozwiązania Dell EMC Avamar DP4400 / Integrated Data Protection Appliance / PowerProtect DP4400 z aktualnej pojemności 16 TB do pojemności docelowej 24 TB.

Rozbudowa musi zwiększyć aktywną pojemność użytkową rozwiązania ochrony danych o 8 TB, bez utraty danych, bez utraty konfiguracji polityk backupu, bez obniżenia dostępności usług backupu i odtwarzania oraz bez utraty wsparcia producenta Dell.

1.2.12.3.2. Cel rozbudowy

Celem zadania jest zwiększenie dostępnej przestrzeni repozytorium backupowego wykorzystywanego do ochrony danych systemu RIS, w tym maszyn wirtualnych, komponentów aplikacyjnych, baz danych, konfiguracji systemowych oraz innych zasobów objętych politykami backupu.

Rozbudowa musi umożliwić dalsze wykonywanie kopii zapasowych w wymaganym okresie retencji, przy zachowaniu integralności danych, deduplikacji, mechanizmów monitorowania, raportowania oraz procedur odtwarzania.

1.2.12.3.3. Weryfikacja stanu istniejącego

Przed dostawą i aktywacją rozbudowy Generalny Wykonawca wykona inwentaryzację posiadanego rozwiązania DP4400, obejmującą co najmniej:

1) identyfikację modelu, wariantu pojemnościowego i numeru seryjnego urządzenia;
2) potwierdzenie aktualnej pojemności licencjonowanej 16 TB;
3) potwierdzenie możliwości rozbudowy do pojemności 24 TB w ramach ścieżki wspieranej przez Dell;
4) identyfikację wersji oprogramowania appliance, Avamar, Data Domain / Protection Storage, Appliance Configuration Manager oraz pozostałych komponentów rozwiązania;
5) weryfikację aktywnego poziomu wsparcia serwisowego Dell;
6) weryfikację stanu zdrowia urządzenia, komponentów sprzętowych, usług i repozytorium backupowego;
7) weryfikację bieżącego wykorzystania pojemności, poziomu deduplikacji, trendu przyrostu danych oraz dostępnej pojemności wolnej;
8) weryfikację aktywnych polityk backupu, harmonogramów, retencji i zadań replikacji, jeżeli są wykorzystywane;
9) weryfikację, czy rozbudowa wymaga wyłącznie aktywacji licencji ELMS, czy dodatkowego pakietu serwisowego, aktualizacji albo działania producenta.

Generalny Wykonawca przedstawi Zamawiającemu raport z inwentaryzacji oraz jednoznaczne potwierdzenie, że oferowany zakres jest właściwy dla konkretnego urządzenia Zamawiającego.

1.2.12.3.4. Wymagania dotyczące dostawy

Generalny Wykonawca dostarczy wszystkie komponenty niezbędne do rozbudowy pojemności rozwiązania DP4400 z 16 TB do 24 TB.

1) Zakres dostawy musi obejmować co najmniej:
2) licencję pojemnościową Dell umożliwiającą zwiększenie aktywnej pojemności urządzenia o 8 TB albo osiągnięcie docelowego progu 24 TB;
3) plik licencyjny ELMS albo inny mechanizm aktywacyjny wymagany przez Dell dla posiadanego urządzenia;
4) usługi aktywacji licencji i konfiguracji rozbudowy;
5) aktualizacje, poprawki, pakiety serwisowe albo inne komponenty programowe wymagane przez Dell do bezpiecznego wykonania rozbudowy;
6) wsparcie producenta Dell albo autoryzowanego partnera Dell w zakresie wymaganym do przeprowadzenia rozbudowy;

7) dokumentację potwierdzającą legalność, oryginalność i zgodność dostarczonej licencji z urządzeniem Zamawiającego.
8) Jeżeli dla konkretnego numeru seryjnego urządzenia Dell wymaga dodatkowego pakietu sprzętowego, serwisowego albo aktualizacyjnego, Generalny Wykonawca musi dostarczyć ten pakiet w ramach wynagrodzenia i uwzględnić go w planie wdrożenia.

1.2.12.3.5. Wymagania dotyczące licencji

Dostarczona licencja musi spełniać co najmniej następujące wymagania:

1) musi pochodzić z legalnego kanału dystrybucji Dell;
2) musi być przypisana albo możliwa do przypisania do posiadanego przez Zamawiającego urządzenia DP4400;
3) musi umożliwiać rozbudowę z aktualnej pojemności 16 TB do pojemności docelowej 24 TB;
4) musi być zgodna z aktualną wersją oprogramowania urządzenia albo z wersją, do której urządzenie zostanie zaktualizowane w ramach zadania;
5) musi być aktywowana w sposób zgodny z procedurą Dell;
6) nie może ograniczać aktualnego wsparcia serwisowego urządzenia;
7) nie może wymagać migracji danych do innego urządzenia ani przebudowy istniejącego środowiska backupowego;
8) musi zostać uwzględniona w dokumentacji licencyjnej przekazanej Zamawiającemu.

Generalny Wykonawca przed aktywacją licencji przedstawi Zamawiającemu potwierdzenie, że licencja odpowiada właściwemu progowi pojemnościowemu i nie spowoduje ograniczenia funkcji urządzenia.

1.2.12.3.6. Wymagania dotyczące wykonania rozbudowy

Generalny Wykonawca przeprowadzi rozbudowę zgodnie z procedurą producenta Dell, w szczególności z wykorzystaniem narzędzi Appliance Configuration Manager oraz mechanizmu aktywacji licencji ELMS, o ile taka ścieżka jest właściwa dla posiadanego urządzenia.

Rozbudowa musi obejmować co najmniej:

1) przygotowanie urządzenia do aktywacji nowej pojemności;
2) wykonanie kopii albo eksportu aktualnej konfiguracji rozwiązania;
3) potwierdzenie braku aktywnych alarmów krytycznych przed rozpoczęciem prac;
4) aktywację licencji pojemnościowej;
5) uruchomienie procedury rozszerzenia pojemności;
6) monitorowanie przebiegu procesu rozszerzenia;

7) weryfikację poprawnego zakończenia procesu;
8) potwierdzenie osiągnięcia docelowej pojemności 24 TB;
9) weryfikację poprawnej pracy usług backupu i odtwarzania;
10) weryfikację poprawnej pracy mechanizmów monitorowania i raportowania.

Prace muszą zostać wykonane w uzgodnionym z Zamawiającym oknie serwisowym. Generalny Wykonawca musi przygotować plan prac, plan testów, plan wycofania zmian oraz listę ryzyk technicznych.

1.2.12.3.7. Wymagania dotyczące ciągłości działania

Generalny Wykonawca musi przeprowadzić rozbudowę w sposób minimalizujący wpływ na działanie środowiska backupowego systemu RIS.

Generalny Wykonawca musi zapewnić:

1) brak utraty istniejących kopii zapasowych;
2) brak utraty konfiguracji polityk backupu;
3) brak utraty konfiguracji retencji;
4) brak utraty konfiguracji użytkowników, ról i uprawnień;
5) brak utraty konfiguracji integracji z VMware vSphere, jeżeli jest wykorzystywana;
6) brak utraty konfiguracji raportowania i monitorowania;
7) brak nieuzgodnionego zatrzymania aktywnych zadań backupu;
8) brak negatywnego wpływu na możliwość odtwarzania danych z kopii wykonanych przed rozbudową.

Jeżeli wykonanie rozbudowy wymaga czasowego wstrzymania harmonogramów backupu, Generalny Wykonawca musi uzgodnić to z Zamawiającym i przedstawić sposób wznowienia zadań po zakończeniu prac.

1.2.12.3.8. Wymagania dotyczące aktualizacji oprogramowania

Jeżeli rozbudowa pojemności wymaga aktualizacji oprogramowania DP4400, Generalny Wykonawca musi wykonać ją w ramach zadania.

Aktualizacja musi obejmować wyłącznie wersje wspierane przez Dell dla posiadanego modelu urządzenia oraz aktualnego stanu środowiska. Generalny Wykonawca musi przedstawić Zamawiającemu informację o wersji wyjściowej, wersji docelowej, wymaganych pakietach, zależnościach, czasie trwania aktualizacji i wpływie na dostępność usług.

Generalny Wykonawca nie może wykonać aktualizacji powodującej utratę wsparcia dla wykorzystywanych funkcji, agentów, integracji z VMware albo innych komponentów środowiska Zamawiającego.

1.2.12.3.9. Wymagania dotyczące testów odbiorowych

Generalny Wykonawca przeprowadzi testy odbiorowe potwierdzające poprawność rozbudowy.

Minimalny zakres testów obejmuje:

1) potwierdzenie poprawnego załadowania i aktywacji licencji;
2) potwierdzenie docelowej pojemności 24 TB w interfejsie zarządzającym;
3) potwierdzenie braku alarmów krytycznych po rozbudowie;
4) potwierdzenie poprawnej pracy Appliance Configuration Manager;
5) potwierdzenie poprawnej pracy komponentów Avamar;
6) potwierdzenie poprawnej pracy Protection Storage / Data Domain, jeżeli występuje jako komponent appliance;
7) wykonanie testowego zadania backupu;
8) wykonanie testu odtworzenia wybranego pliku albo testowej maszyny wirtualnej;
9) potwierdzenie działania istniejących polityk backupu;
10) potwierdzenie zachowania dotychczasowych okresów retencji;
11) potwierdzenie widoczności historycznych kopii zapasowych;
12) potwierdzenie poprawnego raportowania pojemności;
13) potwierdzenie poprawnego monitorowania stanu urządzenia;
14) potwierdzenie, że rozbudowa nie wpłynęła negatywnie na dostępność i integralność istniejących danych backupowych.

Warunkiem odbioru jest osiągnięcie pojemności docelowej 24 TB, pozytywne zakończenie testów backupu i odtwarzania oraz brak błędów krytycznych w urządzeniu.

1.2.12.3.10. Wymagania dotyczące dokumentacji powykonawczej

Generalny Wykonawca przekaże Zamawiającemu dokumentację powykonawczą obejmującą co najmniej:

1) opis stanu urządzenia przed rozbudową;
2) opis wykonanych czynności;
3) dane identyfikacyjne urządzenia;
4) dane dostarczonej licencji;

5) potwierdzenie aktywacji licencji;
6) potwierdzenie osiągnięcia pojemności 24 TB;
7) wykaz wersji oprogramowania przed i po wykonaniu prac;
8) opis ewentualnie wykonanych aktualizacji;
9) zrzuty albo raporty z interfejsu zarządzającego potwierdzające stan po rozbudowie;
10) wyniki testów odbiorowych;
11) opis procedury administracyjnej sprawdzania pojemności;
12) opis procedury diagnostycznej w przypadku problemów z pojemnością, licencją albo usługami backupu;
13) zalecenia dotyczące monitorowania przyrostu danych i planowania kolejnych rozbudów;
14) potwierdzenie zachowania wsparcia producenta Dell.

Dokumentacja musi zostać przekazana w wersji edytowalnej oraz PDF.

1.2.12.3.11. Wymagania dotyczące gwarancji i wsparcia

Generalny Wykonawca zapewni wsparcie dla wykonanej rozbudowy, dostarczonej licencji i wykonanych prac konfiguracyjnych.

Wymagania minimalne:

1) dostarczona licencja musi być objęta wsparciem Dell właściwym dla posiadanego urządzenia;
2) wykonane prace muszą zostać objęte gwarancją Generalnego Wykonawcy;
3) Generalny Wykonawca musi usunąć błędy aktywacji, konfiguracji albo integracji ujawnione po odbiorze;
4) rozbudowa nie może ograniczać aktualnego wsparcia producenta dla urządzenia DP4400;
5) Generalny Wykonawca musi zapewnić udział specjalistów posiadających doświadczenie w administracji i rozbudowie Dell EMC Avamar / IDPA / PowerProtect DP Series Appliance.

1.2.12.3.12. Wymagania dotyczące bezpieczeństwa

Generalny Wykonawca musi prowadzić prace z zachowaniem zasad bezpieczeństwa środowiska RIS.

W szczególności Generalny Wykonawca musi:

1) wykonywać prace wyłącznie na podstawie uzgodnionego planu;
2) stosować konta administracyjne udostępnione albo zatwierdzone przez Zamawiającego;
3) nie wykonywać operacji usuwania danych backupowych;

4) nie modyfikować polityk backupu bez zgody Zamawiającego;
5) nie zmieniać haseł, certyfikatów, konfiguracji sieciowej ani integracji bez zgody Zamawiającego;
6) przekazać Zamawiającemu pełny wykaz wykonanych zmian;
7) zachować poufność informacji dotyczących konfiguracji, danych, polityk backupu i architektury środowiska.

1.2.12.3.13. Rezultat końcowy

Rezultatem zadania musi być posiadane przez Zamawiającego rozwiązanie Dell EMC Avamar DP4400 / Integrated Data Protection Appliance / PowerProtect DP4400 rozbudowane z pojemności 16 TB do pojemności 24 TB.

Rozbudowa musi zostać wykonana w sposób wspierany przez Dell, z wykorzystaniem właściwej licencji pojemnościowej, bez utraty danych, bez utraty konfiguracji, bez obniżenia dostępności usług backupu i odtwarzania oraz bez utraty wsparcia producenta.

1.2.13. Wymagania dla ośrodka zapasowego i łącza teleinformatycznego

1.2.13.1. Przedmiot wymagań

Generalny Wykonawca zobowiązany jest zaprojektować, uzgodnić, dostarczyć, wykonać, uruchomić, przetestować i przekazać do eksploatacji rozwiązanie obejmujące ośrodek zapasowy systemu RIS w zewnętrznym Data Center oraz dedykowane światłowodowe łącze teleinformatyczne 6J pomiędzy serwerownią telekomunikacyjną Zamawiającego a lokalizacją zewnętrznego Data Center.

Zakres zadania obejmuje co najmniej:

1) zapewnienie zewnętrznego Data Center spełniającego wymagania PFU;
2) zapewnienie szafy teleinformatycznej typu RACK o wysokości 47U przeznaczonej do kolokacji zasobów infrastrukturalnych Zamawiającego;
3) zapewnienie przyłącza energetycznego dla szafy wraz z układem pomiarowym i licznikiem energii elektrycznej;
4) zaprojektowanie i wykonanie dedykowanego przyłącza światłowodowego 6J pomiędzy lokalizacją Zamawiającego a zewnętrznym Data Center;
5) zapewnienie zakończeń światłowodowych, przełącznic, patch paneli, oznakowania, dokumentacji trasowej i pomiarowej;
6) uruchomienie połączenia, wykonanie testów transmisyjnych, pomiarów optycznych i testów odbiorowych;

7) zapewnienie utrzymania, nadzoru technicznego, serwisu, usuwania awarii oraz dostępności łącza w wymaganym poziomie SLA;
8) zapewnienie finansowania przez Generalnego Wykonawcę kosztów najmu szafy, zużycia energii elektrycznej, utrzymania infrastruktury, dzierżawy albo korzystania z zasobów niezbędnych do świadczenia usługi transmisji danych, opłat eksploatacyjnych, opłat za umieszczenie infrastruktury w działkach oraz innych kosztów niezbędnych do działania ośrodka zapasowego i łącza w okresie realizacji zamówienia oraz w okresie gwarancji po Odbiorze Końcowym.

1.2.13.2. Cel utworzenia ośrodka zapasowego

Ośrodek zapasowy musi zapewniać warunki techniczne do realizacji funkcji ciągłości działania systemu RIS, odtworzenia po awarii, replikacji danych oraz bezpiecznego przechowywania zasobów infrastrukturalnych i danych Zamawiającego.

Rozwiązanie musi umożliwiać w szczególności:

1) realizację replikacji danych pomiędzy zasobami zlokalizowanymi w serwerowni głównej i ośrodku zapasowym;
2) przechowywanie kopii lub replik danych, konfiguracji i zasobów systemowych wymaganych dla działania systemu RIS;
3) obsługę scenariuszy odtworzeniowych wynikających z Planu Odtworzenia po Awarii DRP;
4) wsparcie scenariuszy ciągłości działania wynikających z Planu Ciągłości Działania BCP;
5) ograniczenie skutków awarii serwerowni głównej, awarii infrastruktury lokalnej, awarii zasobów pamięci masowej albo niedostępności podstawowej lokalizacji systemu RIS;
6) zapewnienie bezpiecznej komunikacji pomiędzy serwerownią główną i zapasową;
7) zapewnienie możliwości monitorowania dostępności, parametrów transmisji, statusu infrastruktury i zdarzeń eksploatacyjnych.

1.2.13.3. Wymagania dotyczące zewnętrznego Data Center

Zewnętrzne Data Center, w którym zostanie utworzony ośrodek zapasowy systemu RIS, musi być profesjonalnym ośrodkiem przetwarzania danych przeznaczonym do świadczenia usług kolokacji infrastruktury teleinformatycznej o znaczeniu krytycznym dla działania systemów informatycznych. Ośrodek musi spełniać wymagania co najmniej odpowiadające poziomowi Tier III albo równoważnemu w zakresie dostępności, redundancji, odporności infrastruktury technicznej, możliwości prowadzenia prac serwisowych bez konieczności wyłączenia usług oraz ograniczenia ryzyka pojedynczego punktu awarii.

Ośrodek zapasowy musi być zlokalizowany w odległości umożliwiającej realizację funkcji replikacji danych pomiędzy zasobami pamięci masowej rozlokowanymi w serwerowni głównej Zamawiającego oraz w zewnętrznym Data Center. Lokalizacja musi umożliwiać uzyskanie parametrów transmisyjnych wymaganych dla replikacji, synchronizacji, backupu, odtwarzania

danych, monitoringu oraz komunikacji administracyjnej pomiędzy lokalizacją podstawową i zapasową.

Zewnętrzne Data Center musi posiadać wdrożony, utrzymywany i stosowany system zarządzania bezpieczeństwem informacji zgodny z ISO/IEC 27001 albo równoważnym standardem bezpieczeństwa informacji. Wymaganie obejmuje co najmniej istnienie formalnych polityk, procedur, mechanizmów kontroli dostępu, zarządzania ryzykiem, zarządzania incydentami, zarządzania zmianą, nadzoru nad dostawcami, rejestrowania zdarzeń oraz okresowego przeglądu środków bezpieczeństwa stosowanych dla usług kolokacyjnych i infrastruktury Data Center.

Ośrodek musi zapewniać redundancję podstawowych systemów technicznych niezbędnych do ciągłej pracy infrastruktury teleinformatycznej, w szczególności zasilania, chłodzenia, dystrybucji energii, monitoringu środowiskowego, systemów bezpieczeństwa fizycznego oraz systemów ochrony przeciwpożarowej. Redundancja ta musi odpowiadać co najmniej wymaganiom klasy Tier III albo rozwiązaniu równoważnemu, zapewniającemu możliwość prowadzenia planowych prac utrzymaniowych bez przerwania świadczenia usług kolokacyjnych dla Zamawiającego.

Data Center musi zapewniać zasilanie podstawowe oraz zasilanie rezerwowe, obejmujące co najmniej system zasilania gwarantowanego UPS oraz źródło zasilania awaryjnego umożliwiające podtrzymanie pracy infrastruktury w przypadku zaniku zasilania podstawowego. System zasilania musi być monitorowany, objęty procedurami utrzymaniowymi i testami okresowymi oraz dostosowany do ciągłej pracy urządzeń teleinformatycznych zainstalowanych w szafie Zamawiającego.

Data Center musi zapewniać system chłodzenia przeznaczony do pracy ciągłej, o parametrach odpowiednich dla infrastruktury teleinformatycznej instalowanej w szafie Zamawiającego. System chłodzenia musi być redundantny albo równoważnie zabezpieczony przed awarią pojedynczego elementu, monitorowany oraz utrzymywany w sposób zapewniający stabilne warunki środowiskowe, w szczególności w zakresie temperatury, wilgotności i przepływu powietrza.

Data Center musi zapewniać ochronę fizyczną infrastruktury Zamawiającego, obejmującą co najmniej kontrolę dostępu do obiektu, kontrolę dostępu do stref technicznych, rejestrację wejść i wyjść, monitoring wizyjny, nadzór nad dostępem serwisowym, ewidencję osób uprawnionych oraz procedury dopuszczania osób trzecich do stref, w których znajduje się infrastruktura Zamawiającego. Dostęp do szafy Zamawiającego musi być możliwy wyłącznie dla osób upoważnionych przez Zamawiającego albo działających na podstawie upoważnienia zaakceptowanego przez Zamawiającego.

Data Center musi być wyposażone w systemy detekcji i sygnalizacji pożaru, rozwiązania ograniczające skutki pożaru oraz procedury reagowania na zdarzenia pożarowe. Zastosowane środki ochrony przeciwpożarowej muszą być adekwatne do charakteru ośrodka przetwarzania danych i nie mogą powodować nieuzasadnionego ryzyka uszkodzenia infrastruktury teleinformatycznej Zamawiającego.

Data Center musi zapewniać monitoring środowiskowy i techniczny obejmujący co najmniej zasilanie, chłodzenie, temperaturę, wilgotność, alarmy techniczne, zdarzenia bezpieczeństwa fizycznego, zdarzenia związane z dostępem oraz awarie infrastruktury krytycznej dla świadczenia usługi kolokacji. Informacje o zdarzeniach mających wpływ na infrastrukturę Zamawiającego muszą być przekazywane w trybie uzgodnionym z Zamawiającym i uwzględnione w procedurach eksploatacyjnych, BCP oraz DRP systemu RIS.

Data Center musi zapewniać warunki techniczne i organizacyjne umożliwiające utrzymanie wymaganej dostępności usług kolokacyjnych oraz infrastruktury transmisyjnej w okresie realizacji zamówienia i w okresie gwarancji po Odbiorze Końcowym. Warunki te muszą obejmować co najmniej procedury obsługi awarii, procedury eskalacji, informowanie o pracach planowych, nadzór techniczny, obsługę zgłoszeń, dostęp serwisowy, okresowe przeglądy oraz utrzymanie dokumentacji eksploatacyjnej.

Generalny Wykonawca zobowiązany jest wykazać, że wskazane Data Center spełnia wymagania określone w niniejszym PFU. Wykazanie spełnienia wymagań może nastąpić w szczególności przez przedstawienie dokumentacji technicznej ośrodka, opisów stosowanych zabezpieczeń, certyfikatów, oświadczeń operatora Data Center, dokumentów potwierdzających zgodność z ISO/IEC 27001 albo standardem równoważnym, dokumentów potwierdzających poziom dostępności odpowiadający co najmniej Tier III albo równoważny oraz dokumentów potwierdzających zasady świadczenia usług kolokacyjnych.

Nie dopuszcza się utworzenia ośrodka zapasowego w lokalizacji, która nie spełnia minimalnych wymagań dotyczących klasy Data Center, bezpieczeństwa informacji, kontroli dostępu, redundancji zasilania, redundancji chłodzenia, ochrony przeciwpożarowej, monitoringu, dostępności usług kolokacyjnych oraz warunków eksploatacji infrastruktury teleinformatycznej o znaczeniu krytycznym dla systemu RIS.

1.2.13.4. Wymagania dotyczące lokalizacji zewnętrznego Data Center

Zewnętrzne Data Center musi być zlokalizowane w odległości umożliwiającej realizację funkcji replikacji danych pomiędzy zasobami pamięci masowej rozlokowanymi w serwerowni głównej Zamawiającego oraz w ośrodku zapasowym. Lokalizacja musi zapewniać warunki do utrzymania wymaganych parametrów transmisji, w szczególności przepustowości, opóźnień, stabilności połączenia, bezpieczeństwa i dostępności.

Zewnętrzne Data Center musi spełniać co najmniej następujące wymagania:

1) zapewniać całoroczną, ciągłą pracę infrastruktury teleinformatycznej;
2) posiadać kontrolowany dostęp fizyczny do stref technicznych, w których będzie kolokowana infrastruktura Zamawiającego;
3) zapewniać możliwość autoryzowanego dostępu serwisowego dla uprawnionych przedstawicieli Zamawiającego, Generalnego Wykonawcy oraz podmiotów utrzymaniowych działających na rzecz Zamawiającego;
4) zapewniać rejestrowanie wejść, wyjść i czynności wykonywanych w strefach technicznych;
5) posiadać system monitoringu fizycznego, system kontroli dostępu, zabezpieczenia przeciwpożarowe oraz procedury reagowania na zdarzenia;
6) zapewniać warunki środowiskowe właściwe dla pracy infrastruktury teleinformatycznej, w szczególności kontrolę temperatury, wilgotności i przepływu powietrza;
7) zapewniać system chłodzenia o parametrach odpowiednich dla pracy urządzeń zainstalowanych w szafie Zamawiającego;

8) zapewniać zasilanie podstawowe i rezerwowe o parametrach właściwych dla infrastruktury teleinformatycznej;
9) zapewniać możliwość eksploatacji szafy RACK 47U z wyposażeniem Zamawiającego;
10) zapewniać możliwość doprowadzenia i zakończenia dedykowanego przyłącza światłowodowego 6J;
11) zapewniać warunki do rozliczania zużycia energii elektrycznej na podstawie dedykowanego układu pomiarowego albo innego mechanizmu zaakceptowanego przez Zamawiającego;
12) zapewniać monitoring techniczny infrastruktury Data Center w zakresie mającym wpływ na pracę zasobów Zamawiającego;
13) zapewniać procedury obsługi incydentów, awarii, prac planowych, okien serwisowych i eskalacji zgłoszeń;
14) umożliwiać utrzymanie wymaganej dostępności usług kolokacyjnych i transmisyjnych w okresie realizacji zamówienia oraz w okresie gwarancji po Odbiorze Końcowym.

Zewnętrzne Data Center musi być obiektem przeznaczonym do profesjonalnej kolokacji infrastruktury teleinformatycznej. Nie dopuszcza się lokalizacji ośrodka zapasowego w pomieszczeniu biurowym, gospodarczym, magazynowym, technicznym albo innym miejscu nieprzeznaczonym do ciągłej eksploatacji infrastruktury teleinformatycznej o znaczeniu krytycznym dla działania systemu RIS.

1.2.13.5. Wymagania dotyczące szafy RACK i kolokacji zasobów Zamawiającego

Generalny Wykonawca zobowiązany jest zapewnić w zewnętrznym Data Center 1 szafę teleinformatyczną typu RACK o wysokości 47U, przeznaczoną do kolokacji zasobów infrastrukturalnych Zamawiającego.

Szafa musi spełniać co najmniej następujące wymagania:

1) wysokość użytkowa 47U;
2) konstrukcja przeznaczona do montażu urządzeń teleinformatycznych w standardzie 19 cali;
3) możliwość zamknięcia i kontroli dostępu do szafy;
4) możliwość prowadzenia okablowania zasilającego i teleinformatycznego w sposób uporządkowany, identyfikowalny i zgodny z dobrą praktyką Data Center;
5) możliwość instalacji przełącznic światłowodowych, paneli krosowych, listew zasilających, urządzeń sieciowych, serwerowych, storage albo innych zasobów Zamawiającego przewidzianych w dokumentacji projektowej;
6) zapewnienie właściwego przepływu powietrza oraz zgodności z organizacją zimnych i ciepłych stref, jeżeli taki model funkcjonuje w Data Center;

7) oznakowanie szafy oraz zainstalowanego wyposażenia zgodnie z przyjętym systemem identyfikacji Zamawiającego.

Generalny Wykonawca musi zapewnić Zamawiającemu prawo korzystania z szafy w okresie realizacji zamówienia oraz w okresie gwarancji po Odbiorze Końcowym, w zakresie niezbędnym do realizacji funkcji ośrodka zapasowego systemu RIS.

1.2.13.6. Wymagania dotyczące zasilania i rozliczania energii elektrycznej

Szafa RACK przeznaczona dla Zamawiającego musi zostać wyposażona w przyłącze energetyczne zapewniające zasilanie urządzeń kolokowanych w ośrodku zapasowym. Parametry przyłącza muszą zostać dobrane na podstawie bilansu energetycznego urządzeń przewidzianych do instalacji, z uwzględnieniem rezerwy rozwojowej i wymagań producentów urządzeń.

Generalny Wykonawca musi zapewnić układ pomiarowy umożliwiający rozliczanie kosztów zużycia energii elektrycznej przez urządzenia Zamawiającego. Układ pomiarowy musi umożliwiać identyfikację zużycia energii przypisanego do szafy Zamawiającego albo do zasobów Zamawiającego w sposób zaakceptowany przez Zamawiającego.

W okresie realizacji przedmiotu zamówienia oraz w okresie gwarancji po Odbiorze Końcowym Generalny Wykonawca zobowiązany jest pokrywać koszty zużycia energii elektrycznej przez zasoby Zamawiającego kolokowane w zewnętrznym Data Center, o ile umowa nie stanowi inaczej.

1.2.13.7. Wymagania dotyczące przyłącza światłowodowego 6J

Generalny Wykonawca zobowiązany jest zaprojektować i wykonać dedykowane światłowodowe przyłącze teleinformatyczne 6J pomiędzy serwerownią telekomunikacyjną Zamawiającego a lokalizacją zewnętrznego Data Center.

Przyłącze światłowodowe 6J musi obejmować co najmniej:

1) opracowanie dokumentacji projektowej;
2) wykonanie inwentaryzacji i analizy możliwej trasy przebiegu kabla;
3) uzyskanie warunków technicznych, zgód, uzgodnień i pozwoleń wymaganych do realizacji trasy;
4) uzyskanie tytułów prawnych, zgód właścicieli, zarządców nieruchomości, zarządców dróg, zarządców kanalizacji kablowej, operatorów infrastruktury albo innych podmiotów, jeżeli są wymagane;

5) wykonanie infrastruktury kablowej, w tym kanalizacji, mikrokanalizacji, rurociągów kablowych, studni, przejść, przepustów, wciągnięcia kabla do istniejącej infrastruktury albo innych elementów wymaganych dla przyjętej technologii;
6) dostawę i instalację kabla światłowodowego 6J;
7) wykonanie zakończeń światłowodowych w serwerowni telekomunikacyjnej Zamawiającego i w zewnętrznym Data Center;
8) instalację przełącznic, patch paneli, adapterów, kaset, osłon, oznaczeń i dokumentacji połączeń;
9) wykonanie pomiarów optycznych wszystkich włókien;
10) wykonanie testów ciągłości, tłumienności, reflektometrycznych i eksploatacyjnych;
11) uruchomienie połączenia transmisyjnego pomiędzy lokalizacjami;
12) przekazanie dokumentacji powykonawczej, pomiarowej, trasowej, własnościowej, gwarancyjnej i eksploatacyjnej.

Przyłącze musi zostać wykonane jako rozwiązanie umożliwiające wykorzystanie wszystkich włókien zgodnie z potrzebami Zamawiającego, w szczególności dla transmisji danych, replikacji, zarządzania, monitoringu, backupu, synchronizacji, testów oraz przyszłej rozbudowy.

Generalny Wykonawca musi zapewnić, aby wszystkie włókna były zakończone, oznakowane, pomierzone i udokumentowane. Dokumentacja musi umożliwiać jednoznaczną identyfikację każdego włókna, toru, zakończenia, przełącznicy, punktu pośredniego i przebiegu trasy.

1.2.13.8. Własność przyłącza światłowodowego

W wyniku realizacji zadania Zamawiający ma stać się właścicielem wybudowanego przyłącza światłowodowego 6J pomiędzy serwerownią telekomunikacyjną Zamawiającego a lokalizacją zewnętrznego Data Center.

Generalny Wykonawca musi zapewnić, aby dokumentacja formalnoprawna, powykonawcza i odbiorowa umożliwiała Zamawiającemu korzystanie z przyłącza w całym wymaganym okresie eksploatacji, w tym jego utrzymanie, serwisowanie, modernizację, rozbudowę oraz dochodzenie uprawnień gwarancyjnych.

Jeżeli trasa przyłącza wykorzystuje infrastrukturę należącą do osób trzecich, Generalny Wykonawca zobowiązany jest wskazać zakres własności Zamawiającego, zakres praw do korzystania z infrastruktury obcej, okres obowiązywania praw, koszty cykliczne, ograniczenia eksploatacyjne oraz warunki utrzymania. Informacje te muszą zostać przedstawione Zamawiającemu przed odbiorem przyłącza.

1.2.13.9. Wymagania dotyczące parametrów transmisyjnych i replikacji danych

Łącze pomiędzy serwerownią główną a ośrodkiem zapasowym musi zostać zaprojektowane z uwzględnieniem funkcji replikacji danych pomiędzy zasobami pamięci masowej rozlokowanymi w obu lokalizacjach. Generalny Wykonawca zobowiązany jest określić wymagane parametry transmisyjne na podstawie docelowej architektury systemu RIS, wolumenu replikowanych danych, zakładanych okien replikacji, wymagań RPO i RTO, wymagań backupu, wymagań aplikacyjnych oraz wymagań bezpieczeństwa.

Projekt musi określać co najmniej:

1) wymaganą przepustowość łącza;
2) dopuszczalne opóźnienia;
3) dopuszczalną zmienność opóźnienia;
4) wymagania dotyczące utraty pakietów;
5) model separacji ruchu pomiędzy replikacją, backupem, administracją, monitoringiem i ruchem usługowym;
6) wymagania dotyczące szyfrowania transmisji;
7) sposób monitorowania parametrów połączenia;
8) sposób alarmowania o degradacji parametrów;
9) sposób testowania replikacji danych;
10) wpływ awarii łącza na pracę systemu RIS;
11) procedury ponownej synchronizacji po przerwie w transmisji.

Łącze nie może być projektowane wyłącznie jako ogólna usługa dostępu do sieci. Musi być zaprojektowane jako dedykowany element architektury odpornościowej systemu RIS, wspierający replikację, odtwarzanie, backup, monitoring i zarządzanie środowiskiem.

1.2.13.10. Wymagania dotyczące bezpieczeństwa

Komunikacja pomiędzy serwerownią główną i ośrodkiem zapasowym musi być realizowana w sposób bezpieczny, kontrolowany i monitorowany. Generalny Wykonawca musi uwzględnić wymagania dotyczące segmentacji sieci, separacji ruchu, kontroli dostępu, szyfrowania transmisji, rejestrowania zdarzeń, monitoringu, zarządzania uprawnieniami oraz ochrony przed nieuprawnionym dostępem.

Wymagania bezpieczeństwa muszą obejmować co najmniej:

1) separację ruchu związanego z replikacją danych od innych klas ruchu, jeżeli wynika to z projektu technicznego;

2) szyfrowanie transmisji albo zastosowanie innego mechanizmu ochrony poufności i integralności danych zaakceptowanego przez Zamawiającego;
3) kontrolę dostępu administracyjnego do urządzeń i usług wykorzystywanych w połączeniu;
4) rejestrowanie zmian konfiguracyjnych;
5) rejestrowanie zdarzeń bezpieczeństwa i zdarzeń eksploatacyjnych;
6) ochronę urządzeń brzegowych przed nieuprawnionym dostępem;
7) zgodność z politykami bezpieczeństwa Zamawiającego;
8) uwzględnienie połączenia i ośrodka zapasowego w dokumentacji cyberbezpieczeństwa systemu RIS;
9) uwzględnienie połączenia i ośrodka zapasowego w procedurach BCP, DRP, backupu, odtwarzania i obsługi incydentów.

1.2.13.11. Wymagania dotyczące utrzymania, kosztów i SLA

W okresie realizacji przedmiotu zamówienia oraz w okresie gwarancji po Odbiorze Końcowym Generalny Wykonawca zobowiązany jest pokrywać koszty niezbędne do funkcjonowania ośrodka zapasowego i łącza teleinformatycznego, w szczególności:

1) koszty najmu szafy teleinformatycznej;
2) koszty zużycia energii elektrycznej;
3) koszty utrzymania infrastruktury Data Center w zakresie przypisanym do zasobów Zamawiającego;
4) koszty utrzymania i świadczenia usługi transmisji danych;
5) koszty nadzoru technicznego;
6) koszty usuwania awarii;
7) koszty serwisu i pomiarów;
8) koszty zapewnienia dostępności łącza w ramach SLA;
9) coroczne opłaty za umieszczenie infrastruktury w działce albo w infrastrukturze osób trzecich;
10) inne koszty eksploatacyjne, administracyjne, formalnoprawne lub utrzymaniowe niezbędne do zachowania ciągłości działania ośrodka zapasowego i łącza.

Generalny Wykonawca musi zapewnić SLA dla łącza teleinformatycznego oraz usług kolokacyjnych. SLA musi obejmować co najmniej:

1) deklarowaną dostępność usługi;
2) czas reakcji na awarię;
3) czas usunięcia awarii;
4) sposób zgłaszania awarii;

5) zasady eskalacji;
6) tryb informowania o pracach planowych;
7) sposób monitorowania dostępności;
8) sposób raportowania parametrów usługi;
9) zasady wykonywania pomiarów okresowych;
10) zasady kwalifikowania niedostępności, degradacji parametrów i prac serwisowych.

1.2.13.12. Wymagania dotyczące dokumentacji projektowej i formalnoprawnej

Generalny Wykonawca zobowiązany jest opracować kompletną dokumentację projektową, formalnoprawną i uzgodnieniową dla ośrodka zapasowego oraz przyłącza światłowodowego 6J.

Dokumentacja musi obejmować co najmniej:

1) koncepcję techniczną ośrodka zapasowego;
2) projekt techniczny przyłącza światłowodowego;
3) projekt trasy kabla;
4) wykaz nieruchomości, działek, zarządców, właścicieli i infrastruktury obcej objętej trasą;
5) wykaz wymaganych zgód, pozwoleń, uzgodnień i warunków technicznych;
6) dokumentację uzgodnieniową z właścicielami, zarządcami i operatorami infrastruktury;
7) dokumentację instalacji w serwerowni Zamawiającego;
8) dokumentację instalacji w zewnętrznym Data Center;
9) schematy logiczne i fizyczne połączenia;
10) schematy zakończeń światłowodowych;
11) schematy zasilania i pomiaru energii dla szafy RACK;
12) plan testów i odbiorów;
13) plan uruchomienia;
14) procedurę wycofania zmian;
15) procedury eksploatacyjne, utrzymaniowe i awaryjne.

Generalny Wykonawca nie może rozpocząć robót budowlanych, instalacyjnych ani prac ingerujących w infrastrukturę Zamawiającego, Data Center albo osób trzecich bez uzyskania wymaganych zgód, pozwoleń i akceptacji dokumentacji przez Zamawiającego.

1.2.13.13. Wymagania dotyczące dokumentacji powykonawczej

Po wykonaniu zadania Generalny Wykonawca zobowiązany jest przekazać Zamawiającemu kompletną dokumentację powykonawczą, obejmującą co najmniej:

1) opis wykonanego rozwiązania;
2) dokumentację trasy światłowodu;
3) dokumentację formalnoprawną dotyczącą prawa do korzystania z trasy i infrastruktury;
4) dokumentację potwierdzającą własność albo uprawnienia Zamawiającego do wybudowanego przyłącza;
5) schematy fizyczne i logiczne połączeń;
6) wykaz zakończeń światłowodowych;
7) oznaczenie wszystkich włókien;
8) protokoły pomiarów optycznych;
9) protokoły testów transmisyjnych;
10) protokoły odbioru robót zanikających, jeżeli wystąpiły;
11) dokumentację szafy RACK;
12) dokumentację przyłącza energetycznego i licznika energii;
13) procedury eksploatacji i utrzymania;
14) procedury zgłaszania awarii;
15) dokumentację SLA;
16) wykaz danych kontaktowych do obsługi Data Center i łącza;
17) dokumentację bezpieczeństwa i dostępu;
18) wykaz kont, uprawnień, ról i zasad dostępu, jeżeli mają zastosowanie;
19) zalecenia eksploatacyjne;
20) dokumenty gwarancyjne.

Dokumentacja powykonawcza musi być spójna z dokumentacją systemu RIS, dokumentacją administratora, dokumentacją eksploatacyjną, Planem Ciągłości Działania BCP, Planem Odtworzenia po Awarii DRP oraz dokumentacją sieci transmisji danych.

1.2.13.14. Testy i odbiór

Odbiór ośrodka zapasowego i łącza teleinformatycznego musi zostać poprzedzony testami potwierdzającymi spełnienie wymagań PFU, dokumentacji projektowej oraz wymagań Zamawiającego.

Testy muszą obejmować co najmniej:

1) weryfikację dostępności szafy RACK i warunków kolokacji;
2) weryfikację działania przyłącza energetycznego i układu pomiarowego;
3) weryfikację dostępu serwisowego do Data Center;
4) weryfikację zakończeń światłowodowych w obu lokalizacjach;
5) pomiary optyczne wszystkich włókien;
6) test ciągłości i tłumienności torów światłowodowych;
7) test transmisji pomiędzy lokalizacjami;
8) test monitorowania łącza;
9) test alarmowania o utracie połączenia;
10) test powrotu połączenia po awarii albo symulowanej przerwie;
11) test replikacji danych albo test techniczny potwierdzający gotowość łącza do replikacji danych, jeżeli replikacja danych będzie uruchamiana w ramach tego samego etapu;
12) test komunikacji z systemami monitorowania Zamawiającego;
13) test procedury zgłoszenia awarii i eskalacji;
14) test poprawności dokumentacji powykonawczej względem stanu rzeczywistego.

W ramach odbioru ośrodka zapasowego Generalny Wykonawca zobowiązany jest przedstawić dokumenty potwierdzające, że zewnętrzne Data Center spełnia wymagania określone w PFU, w szczególności wymagania odpowiadające co najmniej poziomowi Tier III albo równoważnemu oraz wymagania dotyczące systemu zarządzania bezpieczeństwem informacji zgodnego z ISO/IEC 27001 albo standardem równoważnym. Dokumenty te muszą zostać przekazane Zamawiającemu przed przystąpieniem do odbioru końcowego ośrodka zapasowego i stanowią jeden z warunków odbioru tej części przedmiotu zamówienia.

Odbiór może zostać dokonany wyłącznie po przekazaniu kompletnej dokumentacji, protokołów pomiarowych, protokołów testowych, dokumentów potwierdzających prawo korzystania z zasobów Data Center, dokumentów potwierdzających zakres własności albo uprawnień Zamawiającego do przyłącza światłowodowego oraz dokumentów potwierdzających obowiązki utrzymaniowe i gwarancyjne Generalnego Wykonawcy.

1.2.13.15. Gwarancja, utrzymanie i przekazanie do eksploatacji

Generalny Wykonawca zobowiązany jest zapewnić gwarancję, serwis i utrzymanie dla ośrodka zapasowego, szafy RACK, przyłącza energetycznego, układu pomiarowego, przyłącza światłowodowego, zakończeń światłowodowych oraz urządzeń i elementów dostarczonych albo wykonanych w ramach zadania.

W okresie gwarancji po Odbiorze Końcowym Generalny Wykonawca zobowiązany jest zapewnić ciągłość działania usług niezbędnych dla funkcjonowania ośrodka zapasowego i łącza, w tym

pokrywanie kosztów najmu, energii, utrzymania, dzierżawy, nadzoru technicznego, serwisu, usuwania awarii, pomiarów oraz opłat cyklicznych związanych z umieszczeniem infrastruktury w działkach albo infrastrukturze osób trzecich.

Przekazanie do eksploatacji musi obejmować co najmniej:

1) przekazanie dokumentacji powykonawczej;
2) przekazanie procedur eksploatacyjnych;
3) przekazanie procedur awaryjnych;
4) przekazanie zasad dostępu do Data Center;
5) przekazanie zasad zgłaszania i eskalacji awarii;
6) przekazanie informacji o kosztach cyklicznych po zakończeniu okresu, w którym koszty ponosi Generalny Wykonawca;
7) szkolenie albo instruktaż dla wskazanych przedstawicieli Zamawiającego;
8) aktualizację dokumentacji systemu RIS, BCP, DRP i dokumentacji eksploatacyjnej w zakresie dotyczącym ośrodka zapasowego i łącza teleinformatycznego.

1.2.13.16. Rezultat końcowy

Rezultatem zadania musi być działający ośrodek zapasowy systemu RIS w zewnętrznym Data Center, obejmujący udostępnioną szafę RACK 47U z przyłączem energetycznym i układem pomiarowym oraz uruchomione dedykowane przyłącze światłowodowe 6J pomiędzy serwerownią telekomunikacyjną Zamawiającego a lokalizacją Data Center.

Rezultatem zadania musi być również zapewnienie Zamawiającemu własności wybudowanego przyłącza światłowodowego 6J albo praw umożliwiających korzystanie z niego zgodnie z celem zamówienia, w zakresie wynikającym z dokumentacji formalnoprawnej, technicznej i powykonawczej zaakceptowanej przez Zamawiającego.

Rozwiązanie musi być gotowe do wykorzystania jako element architektury ciągłości działania i odtworzenia po awarii systemu RIS, zgodnie z wymaganiami PFU, dokumentacją projektową, Planem Ciągłości Działania BCP, Planem Odtworzenia po Awarii DRP oraz dokumentacją eksploatacyjną systemu RIS.

1.2.14. Wymagania dla środowiska pracy zmodernizowanego systemu RIS

Rozdział określa wymagania Zamawiającego dotyczące zaprojektowania, dostarczenia, wdrożenia, skonfigurowania, uruchomienia, przetestowania i przekazania do eksploatacji środowiska pracy zmodernizowanego systemu RIS.

Środowisko pracy zmodernizowanego systemu RIS należy rozumieć jako kompletną, zintegrowaną i gotową do eksploatacji infrastrukturę sprzętowo-systemową, programową, sieciową, bezpieczeństwa, monitorowania, backupu, replikacji i odtwarzania, przeznaczoną do

uruchomienia i utrzymania usług, aplikacji, baz danych, komponentów integracyjnych, systemów operatorskich, systemów monitorowania, usług cyfrowych, API oraz pozostałych komponentów systemu RIS objętych niniejszym zamówieniem.

Wymagania określone w niniejszym rozdziale mają charakter przekrojowy i należy je stosować łącznie z wymaganiami dotyczącymi usług cyfrowych, interoperacyjności, integracji, cyberbezpieczeństwa, monitoringu technicznego, dokumentacji, testów, odbiorów, gwarancji, serwisu i utrzymania, a także z wymaganiami dotyczącymi doposażenia serwerowni głównej, utworzenia ośrodka zapasowego oraz łącza teleinformatycznego pomiędzy lokalizacją podstawową i zapasową.

1.2.14.1. Przedmiot i cel wymagań

Przedmiotem wymagań jest utworzenie nowego środowiska pracy zmodernizowanego systemu RIS, działającego w oparciu o dwie lokalizacje przetwarzania danych, tj. lokalizację podstawową oraz lokalizację zapasową.

Celem utworzenia środowiska pracy zmodernizowanego systemu RIS jest zapewnienie:

1) wydajnej i bezpiecznej pracy usług systemu RIS;
2) wysokiej dostępności komponentów infrastrukturalnych i aplikacyjnych;
3) odporności na awarie pojedynczych komponentów;
4) możliwości odtworzenia działania systemu po awarii;
5) możliwości replikacji danych pomiędzy lokalizacjami;
6) możliwości wykonywania i odtwarzania kopii zapasowych;
7) możliwości monitorowania, zarządzania i dokumentowania pracy środowiska;
8) możliwości dalszej rozbudowy systemu RIS;
9) zapewnienia środowiska dla usług cyfrowych, usług VTT, informacji hydrologicznej i meteorologicznej, integracji z systemami zewnętrznymi oraz API systemu RIS;
10) zapewnienia warunków technicznych do obsługi danych pochodzących z lokalizacji terenowych, podsystemów VHF/AIS/DGNSS, CCTV, czujników hydrologicznych, sensorów meteorologicznych, sieci transmisji danych i monitoringu technicznego.

Utworzenie środowiska pracy zmodernizowanego systemu RIS stanowi odrębny zakres rzeczowy względem doposażenia serwerowni głównej. Doposażenie serwerowni głównej obejmuje rozbudowę wybranych istniejących komponentów infrastruktury Zamawiającego, natomiast środowisko pracy zmodernizowanego systemu RIS musi zostać zaprojektowane jako kompletne rozwiązanie dwulokalizacyjne, obejmujące wszystkie zasoby niezbędne do uruchomienia i eksploatacji zmodernizowanego systemu RIS.

Generalny Wykonawca ponosi odpowiedzialność za osiągnięcie kompletnego rezultatu w postaci środowiska pracy systemu RIS gotowego do uruchomienia produkcyjnego, utrzymania, monitorowania, zabezpieczenia, odtworzenia po awarii oraz dalszej rozbudowy.

1.2.14.2. Docelowa architektura środowiska pracy

Generalny Wykonawca zobowiązany jest zaprojektować środowisko pracy systemu RIS w architekturze dwulokalizacyjnej, obejmującej co najmniej:

1) lokalizację podstawową, w której będą uruchamiane zasadnicze komponenty produkcyjne systemu RIS;
2) lokalizację zapasową, w której będą uruchamiane zasoby umożliwiające replikację danych, przechowywanie kopii lub replik zasobów systemowych, odtworzenie wybranych funkcji systemu po awarii oraz ograniczenie skutków niedostępności lokalizacji podstawowej;
3) połączenie teleinformatyczne pomiędzy lokalizacją podstawową i zapasową;
4) mechanizmy replikacji, backupu, monitorowania, zarządzania, bezpieczeństwa i odtwarzania po awarii.

Architektura środowiska musi zostać zaprojektowana w sposób eliminujący pojedyncze punkty awarii w zakresie adekwatnym do roli danego komponentu w systemie RIS. Dotyczy to w szczególności zasilania, połączeń sieciowych, kart sieciowych, adapterów, urządzeń aktywnych LAN, urządzeń aktywnych SAN albo równoważnych, kontrolerów pamięci masowej, połączeń między lokalizacjami, serwerów, hostów wirtualizacyjnych, usług zarządzania, usług monitorowania, backupu i replikacji.

Generalny Wykonawca zobowiązany jest przedstawić w dokumentacji projektowej docelową architekturę środowiska pracy, obejmującą co najmniej:

1) opis wariantu architektury;
2) rozmieszczenie zasobów pomiędzy lokalizacją podstawową i zapasową;
3) opis warstwy obliczeniowej;
4) opis warstwy wirtualizacji;
5) opis warstwy składowania danych;
6) opis warstwy LAN;
7) opis warstwy SAN albo równoważnej warstwy komunikacji z zasobami składowania danych, jeżeli zostanie zastosowana;
8) opis warstwy backupu i odtwarzania;
9) opis mechanizmów replikacji;
10) opis komunikacji pomiędzy lokalizacjami;
11) opis segmentacji i bezpieczeństwa;
12) opis monitorowania i zarządzania;
13) opis mechanizmów wysokiej dostępności;
14) opis zależności pomiędzy komponentami środowiska;

15) opis sposobu rozbudowy środowiska w przyszłości.

Dopuszcza się zastosowanie modelu ‘active-passive’ albo innego modelu architektonicznego zapewniającego równoważny lub wyższy poziom dostępności, pod warunkiem wykazania przez Generalnego Wykonawcę, że przyjęta architektura spełnia wymagania PFU, jest możliwa do utrzymania przez Zamawiającego, nie powoduje nadmiernej złożoności eksploatacyjnej oraz umożliwia wykonanie testów odbiorowych i testów odtworzeniowych.

1.2.14.3. Analiza istniejących zasobów Zamawiającego

Generalny Wykonawca zobowiązany jest przeprowadzić analizę istniejących zasobów Zamawiającego, które mogą zostać wykorzystane, rozbudowane, zintegrowane albo powiązane z nowym środowiskiem pracy zmodernizowanego systemu RIS.

Analiza musi obejmować co najmniej:

1) serwery fizyczne i kasetowe;
2) środowisko wirtualizacyjne;
3) macierze dyskowe i zasoby pamięci masowej;
4) rozwiązania backupu i odtwarzania;
5) urządzenia LAN;
6) urządzenia SAN albo urządzenia równoważne stosowane do komunikacji z zasobami danych;
7) urządzenia bezpieczeństwa;
8) przełączniki szkieletowe i dostępowe;
9) urządzenia transmisyjne;
10) szafy RACK;
11) zasilanie, UPS, PDU i liczniki energii;
12) klimatyzację i warunki środowiskowe;
13) okablowanie strukturalne i światłowodowe;
14) licencje, subskrypcje i wsparcie producentów;
15) systemy monitorowania;
16) obecne procedury administracyjne, backupowe, odtworzeniowe, utrzymaniowe i bezpieczeństwa.

W dokumentacji projektowej Generalny Wykonawca musi jednoznacznie wskazać:

1) zasoby istniejące wykorzystywane bez zmian;
2) zasoby istniejące rozbudowywane;

3) zasoby istniejące rekonfigurowane;
4) zasoby istniejące integrowane z nowym środowiskiem;
5) zasoby istniejące pozostające poza zakresem wykorzystania;
6) nowe zasoby dostarczane przez Generalnego Wykonawcę;
7) ograniczenia techniczne, licencyjne, gwarancyjne lub eksploatacyjne wynikające z wykorzystania zasobów istniejących;
8) ryzyka wynikające z integracji nowych komponentów z zasobami istniejącymi;
9) sposób ograniczenia zidentyfikowanych ryzyk.

Wykorzystanie zasobów istniejących nie może prowadzić do obniżenia bezpieczeństwa, dostępności, wydajności, trwałości, gwarancji, wsparcia producenta ani możliwości dalszej rozbudowy systemu RIS. Jeżeli wykorzystanie zasobu istniejącego wymaga rozbudowy licencji, aktualizacji oprogramowania, wymiany komponentu, dostawy modułu, zmiany konfiguracji albo wykonania prac dostosowawczych, Generalny Wykonawca zobowiązany jest uwzględnić ten zakres w projekcie i w cenie oferty.

1.2.14.4. Warstwa obliczeniowa i wirtualizacyjna

Środowisko pracy zmodernizowanego systemu RIS musi obejmować warstwę obliczeniową zapewniającą zasoby niezbędne do uruchomienia i eksploatacji wszystkich komponentów systemu RIS objętych zamówieniem.

Warstwa obliczeniowa musi zapewniać co najmniej:

1) możliwość uruchomienia usług produkcyjnych systemu RIS;
2) możliwość uruchomienia komponentów aplikacyjnych, bazodanowych, integracyjnych, operatorskich, monitorujących, administracyjnych i raportowych;
3) możliwość uruchomienia usług API i integracji z systemami zewnętrznymi;
4) możliwość obsługi usług VTT, informacji hydrologicznej i meteorologicznej oraz usług cyfrowych RIS;
5) możliwość obsługi komponentów wspierających integrację z CCTV, VHF/AIS/DGNSS, czujnikami hydrologicznymi, sensorami meteorologicznymi i systemami monitoringu technicznego;
6) wysoką dostępność hostów i usług;
7) możliwość migracji maszyn wirtualnych albo usług pomiędzy hostami, jeżeli wynika to z przyjętej architektury;
8) możliwość wykonywania kopii zapasowych i odtwarzania usług;
9) możliwość monitorowania wykorzystania zasobów;
10) rezerwę zasobów na rozwój systemu w okresie realizacji i gwarancji.

Generalny Wykonawca zobowiązany jest dostarczyć łącznie 6 serwerów fizycznych, po 3 serwery w każdej lokalizacji przetwarzania danych, oraz dobrać ich typy, konfigurację i parametry techniczne w sposób zapewniający spełnienie wymagań systemu RIS.

Jeżeli środowisko będzie wykorzystywać platformę wirtualizacyjną, wszystkie komponenty sprzętowe, firmware, sterowniki i wersje oprogramowania muszą być zgodne z listami kompatybilności producenta platformy wirtualizacyjnej albo producentów właściwych komponentów. Generalny Wykonawca zobowiązany jest dostarczyć wszystkie licencje, subskrypcje, pakiety wsparcia i aktywacje funkcji niezbędne do legalnej i pełnej eksploatacji środowiska przez okres wymagany w PFU i umowie.

Warstwa obliczeniowa musi być zaprojektowana w sposób umożliwiający wykonywanie prac serwisowych, aktualizacji, wymiany komponentów i rozbudowy z minimalizacją wpływu na działanie usług systemu RIS.

1.2.14.4.1. Minimalne wymagania dla serwerów klastra środowiska pracy systemu RIS

Generalny Wykonawca zobowiązany jest dostarczyć, zainstalować, skonfigurować, uruchomić, zintegrować i przekazać do eksploatacji serwery fizyczne stanowiące zasoby obliczeniowe klastra środowiska pracy zmodernizowanego systemu RIS.

Środowisko pracy zmodernizowanego systemu RIS musi zostać zbudowane w oparciu o łącznie 6 serwerów fizycznych, rozmieszczonych w dwóch lokalizacjach przetwarzania danych, tj.:

1) 3 serwery fizyczne w lokalizacji podstawowej;
2) 3 serwery fizyczne w lokalizacji zapasowej.

Liczba serwerów wskazana powyżej stanowi minimalne i wymagane założenie architektoniczne Zamawiającego. Generalny Wykonawca nie jest uprawniony do zaproponowania mniejszej liczby serwerów fizycznych, nawet jeżeli z analizy wydajnościowej wynikałaby techniczna możliwość uruchomienia systemu RIS na mniejszej liczbie jednostek. Dopuszcza się natomiast dostarczenie większej liczby serwerów, jeżeli będzie to uzasadnione przyjętą architekturą, wymaganiami wydajnościowymi, wymaganiami wysokiej dostępności, wymaganiami odtworzenia po awarii, wymaganiami separacji usług albo wymaganiami dalszej rozbudowy systemu RIS.

Zadaniem Generalnego Wykonawcy pozostaje dobór typów, konfiguracji i parametrów technicznych serwerów oraz zasobów obliczeniowych w taki sposób, aby zapewnić prawidłowe działanie zmodernizowanego systemu RIS. Dobór ten musi zostać dokonany na podstawie analizy wymagań systemu RIS, przewidywanej liczby usług, liczby maszyn wirtualnych albo innych jednostek uruchomieniowych, wolumenu danych, liczby użytkowników, liczby integracji, wymagań wydajnościowych, wymagań wysokiej dostępności, wymagań odtworzenia po awarii, wymagań backupu, wymagań replikacji, wymagań monitorowania oraz wymagań skalowalności.

Wymaganie dostarczenia łącznie 6 serwerów fizycznych nie zwalnia Generalnego Wykonawcy z obowiązku zapewnienia odpowiedniej wydajności, pojemności, niezawodności i skalowalności środowiska. Jeżeli minimalna liczba 6 serwerów okaże się niewystarczająca do spełnienia wymagań PFU, Generalny Wykonawca zobowiązany jest dostarczyć większą liczbę serwerów albo serwery o wyższych parametrach, bez dodatkowego wynagrodzenia.

Serwery muszą być fabrycznie nowe, pełnowartościowe, pochodzić z autoryzowanego kanału sprzedaży producenta lub autoryzowanego partnera, być przeznaczone do pracy w środowisku centrum przetwarzania danych oraz być objęte gwarancją i wsparciem producenta przez okres wymagany w PFU i umowie.

Każdy serwer musi spełniać co najmniej następujące wymagania techniczne:

1) architektura procesorowa klasy x86_64, przeznaczona do pracy serwerowej i wspierana przez producenta oferowanej albo wykorzystywanej platformy wirtualizacyjnej;
2) co najmniej dwa procesory serwerowe albo równoważna konfiguracja zapewniająca porównywalną wydajność obliczeniową, niezawodność i możliwość pracy w klastrze;
3) co najmniej 32 fizyczne rdzenie obliczeniowe w każdym serwerze;
4) co najmniej 512 GB pamięci operacyjnej RAM w każdym serwerze, z możliwością dalszej rozbudowy;
5) pamięć RAM z mechanizmami korekcji błędów, właściwa dla zastosowanej platformy serwerowej;
6) redundantne zasilacze typu hot-plug;
7) redundantne wentylatory albo równoważny system chłodzenia właściwy dla pracy ciągłej;
8) możliwość montażu w szafie RACK albo w istniejącej infrastrukturze kasetowej Zamawiającego, jeżeli taka architektura zostanie przyjęta i zaakceptowana;
9) dedykowany kontroler zarządzania poza pasmem, umożliwiający zdalne zarządzanie, monitorowanie, odczyt stanu sprzętu, aktualizację firmware oraz zdalną diagnostykę;
10) moduł bezpieczeństwa sprzętowego, w szczególności TPM albo rozwiązanie równoważne, jeżeli jest wymagane przez przyjętą architekturę bezpieczeństwa;
11) możliwość pracy z mechanizmami UEFI Secure Boot albo równoważnymi mechanizmami bezpiecznego uruchamiania, jeżeli są wspierane przez oferowaną platformę;
12) redundantne połączenia sieciowe do warstwy LAN;
13) redundantne połączenia do warstwy SAN albo równoważnej warstwy komunikacji z zasobami składowania danych, jeżeli taka warstwa zostanie zastosowana;
14) lokalne nośniki rozruchowe albo inne rozwiązanie boot właściwe dla przyjętej architektury, skonfigurowane w sposób odporny na awarię pojedynczego nośnika;
15) możliwość monitorowania stanu procesorów, pamięci, zasilaczy, wentylatorów, dysków, interfejsów sieciowych, interfejsów storage, temperatury, błędów sprzętowych i zdarzeń krytycznych.

Serwery muszą być w pełni kompatybilne z oferowaną albo wykorzystywaną platformą wirtualizacyjną. Generalny Wykonawca zobowiązany jest dostarczyć serwery, adaptery, sterowniki, firmware i pozostałe komponenty znajdujące się na oficjalnych listach kompatybilności producenta platformy wirtualizacyjnej albo producentów właściwych komponentów infrastruktury.

Jeżeli Generalny Wykonawca wykorzystuje istniejącą platformę wirtualizacyjną Zamawiającego, dostarczane serwery muszą być z nią kompatybilne i objęte wsparciem producenta w konfiguracji przewidzianej do wdrożenia. Jeżeli Generalny Wykonawca dostarcza nową platformę wirtualizacyjną albo nowe licencje, zobowiązany jest zapewnić wszystkie licencje, subskrypcje, aktywacje funkcji, wsparcie producenta oraz komponenty zarządzające niezbędne do eksploatacji wszystkich serwerów klastra.

Warstwa obliczeniowa musi umożliwiać co najmniej:

1) pracę w klastrze wysokiej dostępności w każdej z lokalizacji;
2) współpracę lokalizacji podstawowej i zapasowej w ramach przyjętego modelu BCP/DR;
3) automatyczny restart usług albo maszyn wirtualnych po awarii pojedynczego serwera, jeżeli wynika to z funkcji oferowanej platformy;
4) migrację maszyn wirtualnych albo usług pomiędzy serwerami klastra, jeżeli wynika to z przyjętej architektury;
5) prowadzenie prac serwisowych na pojedynczym serwerze bez konieczności całkowitego zatrzymania środowiska;
6) utrzymanie działania usług krytycznych po awarii pojedynczego serwera w danej lokalizacji;
7) monitorowanie wykorzystania zasobów CPU, RAM, sieci i storage;
8) rozbudowę zasobów obliczeniowych i pamięciowych w przyszłości;
9) odtworzenie konfiguracji serwera po awarii;
10) integrację z systemem monitoringu technicznego zasobów RIS.

Rozmieszczenie serwerów po 3 sztuki w każdej lokalizacji ma zapewniać możliwość pracy środowiska w modelu odpornym na awarię pojedynczego serwera, możliwość prowadzenia prac serwisowych, możliwość utrzymania zasobów rezerwowych oraz możliwość realizacji procedur odtworzeniowych zgodnie z przyjętą architekturą BCP/DR. Generalny Wykonawca zobowiązany jest w dokumentacji projektowej wykazać sposób wykorzystania serwerów w obu lokalizacjach, w tym przypisanie ich do klastra, sposób replikacji, sposób przełączania, sposób powrotu do pracy podstawowej oraz zasady monitorowania dostępności zasobów.

Generalny Wykonawca zobowiązany jest dobrać parametry serwerów z uwzględnieniem rzeczywistego zapotrzebowania zmodernizowanego systemu RIS. Minimalne wymagania określone w niniejszym podrozdziale nie stanowią docelowego sizingu systemu i nie zwalniają Generalnego Wykonawcy z obowiązku dostarczenia konfiguracji wyższej, jeżeli będzie to konieczne do spełnienia wymagań PFU.

Serwery muszą być objęte gwarancją producenta przez okres co najmniej równy okresowi gwarancji wymaganemu dla środowiska pracy systemu RIS. Wymaga się świadczenia wsparcia sprzętowego w miejscu instalacji, z czasem reakcji nie dłuższym niż następny dzień roboczy, chyba że PFU albo umowa przewidują krótszy czas reakcji. W przypadku uszkodzenia nośnika danych, nośnik po wymianie pozostaje u Zamawiającego, jeżeli był wykorzystywany do przechowywania danych, konfiguracji, logów albo innych informacji systemu RIS.

Generalny Wykonawca zobowiązany jest objąć serwery testami odbiorowymi. Testy muszą obejmować co najmniej:

1) weryfikację liczby serwerów w lokalizacji podstawowej i zapasowej;
2) weryfikację zgodności konfiguracji serwerów z dokumentacją projektową;
3) weryfikację zgodności serwerów z wymaganiami platformy wirtualizacyjnej;
4) weryfikację poprawności montażu i okablowania;
5) weryfikację redundantnego zasilania;
6) weryfikację połączeń LAN;
7) weryfikację połączeń SAN albo równoważnych;
8) weryfikację działania zarządzania poza pasmem;
9) weryfikację monitorowania stanu sprzętu;
10) weryfikację pracy serwerów w klastrze;
11) weryfikację zachowania środowiska po awarii pojedynczego serwera;
12) weryfikację możliwości prowadzenia prac serwisowych bez całkowitego zatrzymania środowiska;
13) weryfikację kompletności dokumentacji powykonawczej i konfiguracyjnej.

1.2.14.5. Warstwa składowania danych

Środowisko pracy zmodernizowanego systemu RIS musi obejmować warstwę składowania danych zapewniającą przechowywanie danych produkcyjnych, konfiguracyjnych, aplikacyjnych, bazodanowych, integracyjnych, monitorujących, logów, kopii zapasowych oraz innych danych wymaganych do pracy systemu RIS.

Warstwa składowania danych musi zapewniać co najmniej:

1) odpowiednią pojemność użytkową dla danych systemu RIS;
2) odpowiednią wydajność dla usług aplikacyjnych, bazodanowych, integracyjnych i monitorujących;
3) odporność na awarię pojedynczego dysku, kontrolera, ścieżki komunikacyjnej albo innego komponentu, zgodnie z przyjętą architekturą;
4) możliwość replikacji danych pomiędzy lokalizacją podstawową i zapasową;
5) możliwość wykonywania kopii zapasowych;
6) możliwość odtwarzania danych po awarii;
7) możliwość monitorowania stanu pojemności, wydajności, błędów, alarmów i stanu replikacji;
8) separację danych zgodną z wymaganiami bezpieczeństwa i architektury systemu;
9) możliwość dalszej rozbudowy pojemności;

10) dokumentację struktury wolumenów, zasobów, datastore, LUN, udziałów albo innych jednostek logicznych wynikających z przyjętej technologii.

W ramach systemu RIS nie przewiduje się dostawy i wdrożenia macierzy NAS ani bibliotek taśmowych. Generalny Wykonawca nie może przyjąć architektury, w której dostawa macierzy NAS lub biblioteki taśmowej jest elementem wymaganym do spełnienia przedmiotu zamówienia. Jeżeli dla osiągnięcia wymaganej funkcjonalności konieczne jest zastosowanie mechanizmów plikowych, repozytoriów danych, archiwizacji, backupu albo długoterminowego przechowywania danych, muszą one zostać zrealizowane w ramach innych komponentów środowiska, zgodnych z PFU i zaakceptowanych przez Zamawiającego.

Generalny Wykonawca zobowiązany jest wskazać w dokumentacji projektowej sposób składowania poszczególnych kategorii danych systemu RIS, w tym danych aplikacyjnych, baz danych, danych pomiarowych, danych integracyjnych, logów, konfiguracji, kopii zapasowych, danych monitoringu technicznego oraz danych wymaganych przez mechanizmy odtworzeniowe.

1.2.14.5.1. Minimalne wymagania dla macierzy dyskowych środowiska pracy systemu RIS

Generalny Wykonawca zobowiązany jest dostarczyć, zainstalować, skonfigurować, uruchomić, zintegrować i przekazać do eksploatacji macierze dyskowe stanowiące warstwę centralnego składowania danych środowiska pracy zmodernizowanego systemu RIS.

Minimalna architektura warstwy składowania danych musi obejmować co najmniej dwie macierze dyskowe klasy enterprise, z których jedna zostanie zainstalowana w lokalizacji podstawowej, a druga w lokalizacji zapasowej. Macierze muszą umożliwiać realizację mechanizmów replikacji danych pomiędzy lokalizacjami oraz odtworzenie działania usług systemu RIS zgodnie z przyjętą architekturą BCP/DR.

Macierze dyskowe muszą być fabrycznie nowe, pochodzić z autoryzowanego kanału sprzedaży producenta lub autoryzowanego partnera, być przeznaczone do pracy w środowisku centrum przetwarzania danych oraz być objęte gwarancją i wsparciem producenta przez okres wymagany w PFU i umowie.

Macierze muszą spełniać co najmniej następujące wymagania techniczne:

1) architektura dwukontrolerowa, z kontrolerami pracującymi w trybie wysokiej dostępności;
2) redundantne zasilacze typu hot-plug;
3) redundantne wentylatory albo równoważny system chłodzenia;
4) obsługa dysków SSD klasy enterprise;
5) możliwość pracy z mechanizmami RAID albo równoważnymi mechanizmami ochrony danych przed awarią nośników;
6) odporność na awarię co najmniej pojedynczego dysku bez utraty danych i bez zatrzymania pracy macierzy;

7) możliwość wymiany dysków, zasilaczy i innych elementów serwisowych bez konieczności wyłączania macierzy, jeżeli pozwala na to technologia producenta;
8) redundantne ścieżki dostępu z serwerów klastra do zasobów macierzy;
9) obsługa wielościeżkowości dostępu do danych;
10) możliwość tworzenia wolumenów, zasobów logicznych, datastore, LUN albo równoważnych jednostek logicznych właściwych dla przyjętej technologii;
11) możliwość monitorowania pojemności, wydajności, stanu dysków, stanu kontrolerów, stanu zasilania, stanu interfejsów, błędów, alarmów oraz zdarzeń krytycznych;
12) możliwość integracji z systemem monitoringu technicznego zasobów RIS;
13) możliwość wykonywania kopii migawkowych albo równoważnych mechanizmów punktowego zabezpieczenia danych, jeżeli są wymagane przez przyjętą architekturę;
14) możliwość replikacji danych pomiędzy macierzami albo współpracy z mechanizmem replikacji realizowanym na poziomie platformy wirtualizacyjnej, systemu backupu lub innej warstwy zaakceptowanej przez Zamawiającego;
15) możliwość rozbudowy pojemności w przyszłości bez wymiany całej macierzy.

Macierze dyskowe muszą zostać dostarczone w konfiguracji zapewniającej odpowiednią pojemność, wydajność, odporność na awarie nośników, możliwość prowadzenia prac serwisowych oraz możliwość dalszej rozbudowy. Zamawiający wymaga, aby każda macierz dyskowa została wyposażona w co najmniej 12 dysków SSD klasy enterprise, przeznaczonych do pracy ciągłej w środowisku centrum przetwarzania danych.

Dyski zastosowane w macierzach muszą spełniać co najmniej następujące wymagania:

1) typ nośnika: SSD klasy enterprise;
2) interfejs i typ nośników zgodny z architekturą oferowanej macierzy oraz rekomendacjami jej producenta;
3) przeznaczenie do pracy w macierzach dyskowych klasy centrum przetwarzania danych;
4) obsługa pracy ciągłej 24/7;
5) objęcie wsparciem producenta macierzy w oferowanej konfiguracji;
6) możliwość wymiany uszkodzonego nośnika bez wyłączania macierzy, jeżeli funkcja taka jest wspierana przez oferowaną platformę;
7) zgodność z mechanizmami ochrony danych, replikacji, monitorowania, alarmowania i diagnostyki oferowanej macierzy.

Pojemność pojedynczego dysku SSD nie może być mniejsza niż 3,84 TB. Dopuszcza się zastosowanie dysków o większej pojemności, pod warunkiem spełnienia wymagań dotyczących wydajności, odporności, kompatybilności, wsparcia producenta oraz pojemności użytkowej wymaganej dla środowiska pracy systemu RIS.

Każda macierz musi zapewniać pojemność użytkową, po zastosowaniu mechanizmów ochrony danych, nie mniejszą niż 30 TB. Pojemność użytkowa oznacza pojemność dostępną dla systemów, usług, baz danych, maszyn wirtualnych, repozytoriów i pozostałych danych systemu RIS po uwzględnieniu mechanizmów ochrony danych, dysków zapasowych, narzutów technologicznych, replikacji lokalnej, kopii migawkowych oraz innych mechanizmów ograniczających pojemność dostępną dla Zamawiającego.

Generalny Wykonawca zobowiązany jest zapewnić w każdej macierzy co najmniej dwa dyski zapasowy typu hot spare albo równoważny mechanizm automatycznej odbudowy ochrony danych po awarii nośnika, zgodny z architekturą oferowanej macierzy. Mechanizm ten musi umożliwiać rozpoczęcie procesu odbudowy ochrony danych bez konieczności ręcznej rekonfiguracji macierzy przez administratora, o ile funkcja taka jest dostępna w oferowanym rozwiązaniu.

Konfiguracja dysków musi zapewniać odporność na awarię co najmniej jednego dysku bez utraty danych i bez zatrzymania pracy macierzy. Jeżeli Generalny Wykonawca zastosuje mechanizm ochrony danych zapewniający odporność na awarię więcej niż jednego dysku, zostanie to uznane za rozwiązanie korzystniejsze, pod warunkiem zachowania wymaganej pojemności użytkowej i wydajności.

Generalny Wykonawca zobowiązany jest w dokumentacji projektowej przedstawić bilans pojemnościowy i wydajnościowy macierzy, obejmujący co najmniej:

1) liczbę dysków fizycznych;
2) typ dysków;
3) pojemność pojedynczego dysku;
4) pojemność surową macierzy;
5) zastosowany mechanizm ochrony danych;
6) pojemność utraconą na mechanizmy ochrony danych;
7) pojemność przeznaczoną na dyski zapasowe albo mechanizmy równoważne;
8) pojemność przeznaczoną na kopie migawkowe, jeżeli są stosowane;
9) pojemność użytkową dostępną dla systemu RIS;
10) rezerwę pojemności;
11) zakładany wzrost danych w okresie gwarancji;
12) przewidywaną wydajność macierzy dla obciążeń systemu RIS;
13) sposób zapewnienia replikacji danych pomiędzy lokalizacjami.

Minimalna liczba dysków, minimalny typ dysków i minimalna pojemność pojedynczego dysku określone w niniejszym podrozdziale nie zwalniają Generalnego Wykonawcy z obowiązku dostarczenia konfiguracji o większej liczbie dysków, większej pojemności albo wyższej wydajności, jeżeli będzie to konieczne do spełnienia wymagań systemu RIS, wymagań wysokiej dostępności, wymagań odtwarzania po awarii, wymagań replikacji, wymagań backupu albo wymagań skalowalności.

Każda macierz musi zapewniać pojemność użytkową, po zastosowaniu wybranego mechanizmu ochrony danych, nie mniejszą niż wynikająca z bilansu pojemnościowego opracowanego przez Generalnego Wykonawcę i zaakceptowanego przez Zamawiającego. Bilans pojemnościowy musi uwzględniać co najmniej:

1) dane aplikacyjne systemu RIS;
2) bazy danych;
3) dane pomiarowe;
4) dane integracyjne;
5) dane konfiguracyjne;
6) dane systemów monitorowania;
7) logi;
8) repozytoria techniczne;
9) dane wymagane dla usług cyfrowych, API i integracji zewnętrznych;
10) mechanizmy kopii migawkowych, jeżeli zostaną zastosowane;
11) replikację danych pomiędzy lokalizacjami;
12) wzrost wolumenu danych w okresie gwarancji;
13) rezerwę pojemności na rozwój systemu.

Macierze muszą być kompatybilne z oferowaną albo wykorzystywaną platformą wirtualizacyjną, systemem backupu, mechanizmami replikacji, urządzeniami SAN albo równoważną warstwą komunikacji z zasobami danych oraz systemem monitoringu technicznego. Generalny Wykonawca zobowiązany jest potwierdzić zgodność macierzy, kontrolerów, dysków, firmware, sterowników, adapterów i oprogramowania zarządzającego z listami kompatybilności producentów właściwych komponentów.

Macierze muszą umożliwiać bezpieczne zarządzanie administracyjne, w szczególności:

1) kontrolę dostępu administratorów;
2) indywidualne konta administracyjne albo integrację z mechanizmem uwierzytelniania zaakceptowanym przez Zamawiającego;
3) logowanie zdarzeń administracyjnych;
4) logowanie błędów i alarmów;
5) możliwość eksportu albo przekazywania zdarzeń do systemu monitoringu;
6) zmianę domyślnych poświadczeń przed przekazaniem do eksploatacji;
7) wykonanie kopii konfiguracji;
8) odtworzenie konfiguracji po awarii albo wymianie komponentu.

Generalny Wykonawca zobowiązany jest dostarczyć wszystkie licencje, aktywacje funkcji, moduły, kable, wkładki, adaptery, szyny montażowe, elementy zasilania, oprogramowanie zarządzające, pakiety wsparcia, dokumentację i inne elementy wymagane do pełnego wykorzystania macierzy w architekturze środowiska pracy systemu RIS.

W ramach systemu RIS nie przewiduje się dostawy i wdrożenia macierzy NAS ani bibliotek taśmowych. Macierze dyskowe, o których mowa w niniejszym podrozdziale, mają pełnić funkcję zasobów centralnego składowania danych środowiska pracy systemu RIS i nie mogą być utożsamiane z macierzami NAS ani bibliotekami taśmowymi wyłączonymi z zakresu zamówienia.

Macierze muszą być objęte gwarancją producenta przez okres co najmniej równy okresowi gwarancji wymaganemu dla środowiska pracy systemu RIS. Wymaga się świadczenia wsparcia sprzętowego w miejscu instalacji, z czasem reakcji nie dłuższym niż następny dzień roboczy, chyba że PFU albo umowa przewidują krótszy czas reakcji. W przypadku uszkodzenia dysku albo innego nośnika danych, nośnik po wymianie pozostaje u Zamawiającego.

Generalny Wykonawca zobowiązany jest objąć macierze dyskowe testami odbiorowymi. Testy muszą obejmować co najmniej:

1) weryfikację kompletności dostawy;
2) weryfikację zgodności konfiguracji z dokumentacją projektową;
3) weryfikację dostępnej pojemności użytkowej;
4) weryfikację mechanizmów ochrony danych;
5) weryfikację wielościeżkowości dostępu do danych;
6) weryfikację komunikacji z serwerami klastra;
7) weryfikację replikacji danych pomiędzy lokalizacjami albo współpracy z mechanizmem replikacji przyjętym w architekturze;
8) weryfikację monitorowania i alarmowania;
9) weryfikację odtworzenia wybranego zasobu albo wolumenu testowego;
10) weryfikację poprawności dokumentacji powykonawczej i konfiguracyjnej.

1.2.14.6. Warstwa LAN, SAN i urządzenia aktywne

Generalny Wykonawca zobowiązany jest zaprojektować i wykonać warstwę komunikacyjną środowiska pracy systemu RIS, obejmującą komunikację LAN, SAN albo równoważną, komunikację zarządzającą, komunikację backupową, komunikację replikacyjną, komunikację pomiędzy lokalizacjami oraz komunikację z istniejącą siecią Zamawiającego.

Dobór liczby, typów, parametrów i konfiguracji przełączników SAN, przełączników LAN oraz innych urządzeń aktywnych niezbędnych do zapewnienia komunikacji komponentów środowiska w ramach poszczególnych lokalizacji oraz pomiędzy nimi należy do obowiązków Generalnego Wykonawcy. Dobór ten musi uwzględniać zasoby posiadane przez Zamawiającego, wymagania dotyczące wydajności, dostępności, redundancji, bezpieczeństwa, segmentacji, separacji ruchu, replikacji, backupu, monitoringu, zarządzania i dalszej rozbudowy.

Warstwa LAN musi zapewniać co najmniej:

1) redundantną komunikację pomiędzy hostami, usługami, systemami aplikacyjnymi, bazami danych, systemami monitoringu, systemami backupu i urządzeniami bezpieczeństwa;
2) separację ruchu produkcyjnego, zarządzającego, backupowego, replikacyjnego, operatorskiego, integracyjnego i administracyjnego, jeżeli wynika to z przyjętej architektury;
3) możliwość definiowania stref, VLAN, podsieci, reguł komunikacji i mechanizmów kontroli dostępu;
4) odpowiednią przepustowość dla usług systemu RIS;
5) odpowiednią przepustowość dla integracji z lokalizacjami terenowymi oraz systemami zewnętrznymi;
6) możliwość monitorowania portów, interfejsów, błędów, wykorzystania, alarmów i zdarzeń;
7) możliwość dalszej rozbudowy liczby portów i przepustowości.

Warstwa SAN albo równoważna warstwa komunikacji z zasobami danych musi zapewniać co najmniej:

1) redundantną komunikację pomiędzy hostami a zasobami pamięci masowej;
2) separację ruchu storage od ruchu produkcyjnego, jeżeli wynika to z przyjętej architektury;
3) odpowiednią przepustowość i opóźnienia dla usług systemu RIS;
4) brak pojedynczego punktu awarii w ścieżkach dostępu do danych;
5) możliwość monitorowania stanu portów, ścieżek, błędów, obciążenia i alarmów;
6) możliwość rozbudowy środowiska bez przebudowy zasadniczej architektury.

Generalny Wykonawca zobowiązany jest dostarczyć wszystkie wkładki optyczne, kable DAC/AOC, patchcordy światłowodowe i miedziane, kable LAN, kable SAN, kable zasilające, elementy montażowe, organizery kablowe, opisy, etykiety, moduły, licencje, aktywacje funkcji i inne akcesoria niezbędne do kompletnego uruchomienia warstwy komunikacyjnej środowiska.

1.2.14.7. Lokalizacja zapasowa i połączenie pomiędzy lokalizacjami

Środowisko pracy zmodernizowanego systemu RIS musi być powiązane z lokalizacją zapasową i łączem teleinformatycznym pomiędzy lokalizacją podstawową i zapasową.

Wymagania szczegółowe dotyczące ośrodka zapasowego, zewnętrznego Data Center, szafy RACK, kolokacji zasobów Zamawiającego, zasilania, rozliczania energii, przyłącza światłowodowego 6J, własności przyłącza, parametrów transmisyjnych, bezpieczeństwa, utrzymania, kosztów, SLA, dokumentacji, testów, gwarancji i przekazania do eksploatacji określono w rozdziale 1.2.13.

Generalny Wykonawca zobowiązany jest zaprojektować środowisko pracy systemu RIS w sposób spójny z wymaganiami rozdziału 1.2.13. Oznacza to, że środowisko pracy nie może być projektowane w oderwaniu od lokalizacji zapasowej, parametrów połączenia między lokalizacjami, możliwości replikacji danych, zasad odtwarzania po awarii, wymagań bezpieczeństwa, monitoringu i kosztów eksploatacyjnych.

Połączenie pomiędzy lokalizacjami musi zostać uwzględnione w projekcie architektury jako element krytyczny dla replikacji danych, kopii zapasowych, synchronizacji konfiguracji, monitorowania, zarządzania, przełączenia awaryjnego i odtworzenia po awarii.

Generalny Wykonawca zobowiązany jest określić w dokumentacji projektowej:

1) które usługi i dane są replikowane do lokalizacji zapasowej;
2) w jakim trybie wykonywana jest replikacja;
3) jakie są wymagania przepustowościowe i opóźnieniowe;
4) jakie są zależności pomiędzy replikacją, backupem i odtwarzaniem po awarii;
5) jakie usługi mogą zostać uruchomione w lokalizacji zapasowej;
6) jaki jest przewidywany tryb przełączenia pracy do lokalizacji zapasowej;
7) jaki jest przewidywany tryb powrotu do lokalizacji podstawowej;
8) jakie czynności wymagają udziału administratora;
9) jakie czynności mogą zostać zautomatyzowane;
10) jakie są ograniczenia przyjętej architektury.

1.2.14.8. Backup, replikacja i odtwarzanie po awarii

Środowisko pracy systemu RIS musi zapewniać mechanizmy wykonywania kopii zapasowych, replikacji oraz odtwarzania po awarii, zgodne z Planem Ciągłości Działania BCP, Planem Odtworzenia po Awarii DRP, wymaganiami bezpieczeństwa, wymaganiami eksploatacyjnymi i wymaganiami Zamawiającego.

Generalny Wykonawca zobowiązany jest zaprojektować i wdrożyć mechanizmy backupu i odtwarzania obejmujące co najmniej:

1) maszyny wirtualne albo inne jednostki uruchomieniowe systemu;
2) bazy danych;
3) konfiguracje aplikacji;
4) konfiguracje urządzeń sieciowych i bezpieczeństwa;
5) konfiguracje usług integracyjnych;
6) konfiguracje API;
7) konfiguracje systemów monitorowania;
8) dane pomiarowe;

9) dane aplikacyjne;
10) dane administracyjne;
11) logi, w zakresie wymaganym przez Zamawiającego;
12) inne dane i konfiguracje niezbędne do odtworzenia działania systemu RIS.

Generalny Wykonawca zobowiązany jest określić w dokumentacji projektowej proponowane parametry RTO i RPO dla poszczególnych kategorii usług, danych i komponentów. Parametry te muszą zostać uzgodnione z Zamawiającym i uwzględnione w Planie Ciągłości Działania BCP oraz Planie Odtworzenia po Awarii DRP.

Mechanizmy backupu i replikacji muszą zostać objęte monitoringiem, logowaniem i alarmowaniem. System musi umożliwiać wykrycie nieudanej kopii, opóźnienia replikacji, przerwania transmisji, błędów odtworzeniowych, niedostępności repozytorium, braku pojemności, błędów integralności oraz innych zdarzeń wpływających na możliwość odtworzenia systemu.

Generalny Wykonawca zobowiązany jest przeprowadzić testy odtworzeniowe przed odbiorem środowiska. Testy muszą potwierdzić możliwość odtworzenia wskazanych usług, danych i konfiguracji zgodnie z zaakceptowanymi procedurami i parametrami.

1.2.14.9. Wysoka dostępność i odporność na awarie

Środowisko pracy zmodernizowanego systemu RIS musi zostać zaprojektowane i wykonane jako środowisko wysokiej dostępności.

Wymagania wysokiej dostępności obejmują co najmniej:

1) redundancję zasilania komponentów krytycznych;
2) redundancję połączeń sieciowych;
3) redundancję połączeń SAN albo równoważnych;
4) redundancję adapterów LAN i SAN albo równoważnych;
5) redundancję urządzeń aktywnych;
6) redundancję ścieżek dostępu do danych;
7) redundancję hostów wirtualizacyjnych;
8) możliwość pracy usług po awarii pojedynczego hosta;
9) możliwość odtworzenia usług po awarii komponentów środowiska;
10) mechanizmy monitorowania i alarmowania o utracie redundancji;
11) procedury serwisowe umożliwiające wymianę komponentów z minimalizacją wpływu na działanie systemu;
12) procedury testowania mechanizmów HA.

Redundancja adapterów, połączeń i urządzeń nie może być realizowana wyłącznie przez zwielokrotnienie portów na pojedynczym komponencie, jeżeli awaria tego komponentu powodowałaby utratę funkcji krytycznej. Generalny Wykonawca zobowiązany jest wykazać w projekcie, że zastosowane rozwiązanie nie zawiera nieuzasadnionych pojedynczych punktów awarii.

Jeżeli z przyczyn technicznych albo ekonomicznych całkowita eliminacja pojedynczego punktu awarii dla wybranego komponentu nie jest możliwa albo racjonalna, Generalny Wykonawca zobowiązany jest wskazać ten komponent, uzasadnić odstępstwo, opisać ryzyko, zaproponować środki ograniczające oraz uzyskać akceptację Zamawiającego.

1.2.14.10. Bezpieczeństwo środowiska

Środowisko pracy zmodernizowanego systemu RIS musi spełniać wymagania cyberbezpieczeństwa, kontroli dostępu, monitoringu i logowania określone w PFU, w szczególności w rozdziale dotyczącym cyberbezpieczeństwa, kontroli dostępu, monitoringu i logowania.

Generalny Wykonawca zobowiązany jest zapewnić co najmniej:

1) segmentację logiczną środowiska;
2) separację ruchu produkcyjnego, zarządzającego, backupowego, replikacyjnego, integracyjnego i administracyjnego;
3) kontrolę dostępu administracyjnego;
4) kontrolę dostępu do platformy wirtualizacyjnej;
5) kontrolę dostępu do urządzeń LAN i SAN;
6) kontrolę dostępu do macierzy lub innych zasobów składowania danych;
7) kontrolę dostępu do systemów backupu i replikacji;
8) kontrolę dostępu do systemów monitorowania;
9) szyfrowanie transmisji administracyjnej i integracyjnej, jeżeli wynika to z charakteru danych lub kanału komunikacji;
10) logowanie działań administracyjnych;
11) logowanie zdarzeń bezpieczeństwa;
12) synchronizację czasu wszystkich komponentów;
13) zabezpieczenie kont technicznych i serwisowych;
14) zmianę domyślnych haseł i usunięcie albo zablokowanie nieużywanych kont;
15) bezpieczne przekazanie poświadczeń Zamawiającemu;
16) możliwość rotacji haseł, kluczy, tokenów i certyfikatów;
17) dokumentowanie konfiguracji bezpieczeństwa;
18) możliwość wykonania kopii konfiguracji komponentów środowiska.

Dostęp zdalny do środowiska pracy systemu RIS może być realizowany wyłącznie w sposób zatwierdzony przez Zamawiającego, kontrolowany, szyfrowany, monitorowany i logowany. Niedopuszczalne jest pozostawienie nieudokumentowanych połączeń serwisowych, tuneli, kont producenta, kont wspólnych albo innych mechanizmów dostępu poza wiedzą i kontrolą Zamawiającego.

1.2.14.11. Monitoring techniczny i zarządzanie środowiskiem

Wszystkie kluczowe komponenty środowiska pracy zmodernizowanego systemu RIS muszą zostać objęte monitoringiem technicznym.

Monitoring musi obejmować co najmniej:

1) dostępność hostów;
2) dostępność maszyn wirtualnych albo równoważnych jednostek uruchomieniowych;
3) stan platformy wirtualizacyjnej;
4) stan zasobów CPU, RAM, dysków i sieci;
5) stan zasobów pamięci masowej;
6) stan urządzeń LAN;
7) stan urządzeń SAN albo równoważnych;
8) stan połączenia pomiędzy lokalizacjami;
9) stan backupu;
10) stan replikacji;
11) stan usług aplikacyjnych;
12) stan usług bazodanowych;
13) stan usług integracyjnych;
14) stan API;
15) stan usług monitoringu;
16) zdarzenia bezpieczeństwa;
17) alarmy producentów urządzeń;
18) wykorzystanie pojemności;
19) wykorzystanie przepustowości;
20) utratę redundancji;
21) awarie komponentów;
22) przekroczenia progów krytycznych i ostrzegawczych.

Monitoring środowiska pracy musi zostać zintegrowany z docelowym albo istniejącym systemem monitorowania zasobów RIS. Jeżeli integracja wymaga dostarczenia dodatkowych licencji, agentów, modułów, konektorów, szablonów monitorowania albo profili urządzeń, Generalny Wykonawca zobowiązany jest dostarczyć je w ramach zamówienia.

Generalny Wykonawca zobowiązany jest przygotować widoki monitoringu, raporty i alarmy umożliwiające ocenę stanu środowiska w podziale na lokalizację podstawową, lokalizację zapasową, warstwę obliczeniową, warstwę składowania danych, warstwę LAN, warstwę SAN, backup, replikację, usługi aplikacyjne, usługi integracyjne i komponenty bezpieczeństwa.

1.2.14.12. Licencje, subskrypcje, wsparcie i aktualizacje

Generalny Wykonawca zobowiązany jest dostarczyć wszystkie licencje, subskrypcje, aktywacje funkcji, certyfikaty, pakiety wsparcia, uprawnienia serwisowe, aktualizacje oprogramowania i firmware oraz inne uprawnienia wymagane do uruchomienia, eksploatacji, monitorowania, zabezpieczenia i utrzymania środowiska pracy zmodernizowanego systemu RIS przez okres wymagany w PFU i umowie.

Wymaganie obejmuje w szczególności:

1) platformę wirtualizacyjną;
2) systemy operacyjne;
3) oprogramowanie bazodanowe, jeżeli jest wymagane dla dostarczanych komponentów;
4) oprogramowanie backupu;
5) mechanizmy replikacji;
6) oprogramowanie zarządzające;
7) oprogramowanie monitorujące;
8) licencje urządzeń LAN;
9) licencje urządzeń SAN albo równoważnych;
10) licencje urządzeń bezpieczeństwa;
11) licencje funkcji wysokiej dostępności;
12) licencje funkcji szyfrowania;
13) licencje funkcji raportowania;
14) licencje wymagane do integracji z istniejącymi systemami Zamawiającego.

Brak licencji, subskrypcji, aktywacji funkcji, modułu albo uprawnienia serwisowego nie może ograniczać możliwości korzystania z funkcji wymaganych w PFU. Wszystkie licencje muszą być

udzielone albo przeniesione w sposób umożliwiający Zamawiającemu legalne korzystanie ze środowiska po odbiorze.

Dostarczane komponenty muszą pochodzić z autoryzowanego kanału sprzedaży producenta albo autoryzowanego partnera, być nowe, pełnowartościowe, nieużywane, niewycofane ze wsparcia producenta, objęte gwarancją i wsparciem producenta oraz dopuszczone do eksploatacji w środowisku produkcyjnym.

1.2.14.13. Kompletność dostawy i wdrożenia

Generalny Wykonawca zobowiązany jest dostarczyć i wdrożyć wszystkie komponenty niezbędne do osiągnięcia wymaganej funkcjonalności środowiska pracy zmodernizowanego systemu RIS, nawet jeżeli dany komponent nie został literalnie wymieniony w PFU, ale jest niezbędny do prawidłowego działania przyjętej architektury.

Zakres kompletności obejmuje w szczególności:

1) sprzęt;
2) oprogramowanie;
3) licencje;
4) subskrypcje;
5) wkładki optyczne;
6) kable DAC/AOC;
7) patchcordy światłowodowe;
8) patchcordy miedziane;
9) kable LAN;
10) kable SAN;
11) kable zasilające;
12) moduły rozszerzeń;
13) karty sieciowe;
14) adaptery;
15) elementy montażowe;
16) organizery kablowe;
17) etykiety i oznaczenia;
18) konfigurację;
19) dokumentację;
20) testy;
21) szkolenie administratorów;
22) przekazanie wiedzy;

23) wsparcie gwarancyjne.

Dostarczone środowisko musi być przekazane Zamawiającemu jako rozwiązanie kompletne, zamontowane, skonfigurowane, opisane, przetestowane, udokumentowane i gotowe do eksploatacji.

1.2.14.14. Dokumentacja środowiska pracy

Generalny Wykonawca zobowiązany jest opracować i przekazać Zamawiającemu kompletną dokumentację środowiska pracy zmodernizowanego systemu RIS.

Dokumentacja musi obejmować co najmniej:

1) opis architektury logicznej;
2) opis architektury fizycznej;
3) opis lokalizacji podstawowej;
4) opis lokalizacji zapasowej;
5) opis rozmieszczenia zasobów pomiędzy lokalizacjami;
6) schematy połączeń LAN;
7) schematy połączeń SAN albo równoważnych;
8) schematy połączeń z pamięcią masową;
9) schematy połączeń między lokalizacjami;
10) schematy zasilania;
11) wykaz sprzętu;
12) wykaz oprogramowania;
13) wykaz licencji;
14) wykaz adresacji;
15) wykaz VLAN, podsieci i stref;
16) wykaz reguł komunikacji;
17) wykaz kont, ról i uprawnień;
18) opis konfiguracji platformy wirtualizacyjnej;
19) opis konfiguracji serwerów;
20) opis konfiguracji pamięci masowej;
21) opis konfiguracji LAN;
22) opis konfiguracji SAN albo równoważnej;
23) opis konfiguracji backupu;
24) opis konfiguracji replikacji;

25) opis konfiguracji HA;
26) opis konfiguracji monitoringu;
27) opis konfiguracji bezpieczeństwa;
28) procedury administracyjne;
29) procedury aktualizacji;
30) procedury backupu;
31) procedury odtwarzania;
32) procedury przełączenia do lokalizacji zapasowej;
33) procedury powrotu do lokalizacji podstawowej;
34) procedury awaryjne;
35) procedury wykonywania kopii konfiguracji;
36) procedury odtworzenia konfiguracji;
37) raport z testów;
38) protokoły odbiorowe;
39) wykaz znanych ograniczeń i zaakceptowanych odstępstw.

Dokumentacja musi być spójna z Dokumentacją Administratora, Dokumentacją Eksploatacyjną systemu RIS, Planem Ciągłości Działania BCP, Planem Odtworzenia po Awarii DRP, Polityką Zarządzania Podatnościami, dokumentacją monitoringu technicznego, dokumentacją cyberbezpieczeństwa, dokumentacją usług cyfrowych oraz dokumentacją integracji.

1.2.14.15. Testy i odbiór środowiska pracy

Generalny Wykonawca zobowiązany jest przygotować i przeprowadzić testy środowiska pracy zmodernizowanego systemu RIS. Testy muszą zostać wykonane na podstawie zaakceptowanej przez Zamawiającego dokumentacji testowej.

Testy muszą obejmować co najmniej:

1) weryfikację kompletności dostawy;
2) weryfikację dostarczenia łącznie 6 serwerów fizycznych, w tym 3 serwerów w lokalizacji podstawowej i 3 serwerów w lokalizacji zapasowej;
3) weryfikację zgodności dostarczonych komponentów z dokumentacją projektową;
4) weryfikację montażu;
5) weryfikację okablowania;
6) weryfikację oznakowania;
7) weryfikację konfiguracji serwerów;
8) weryfikację konfiguracji platformy wirtualizacyjnej;

9) weryfikację konfiguracji pamięci masowej;
10) weryfikację konfiguracji LAN;
11) weryfikację konfiguracji SAN albo równoważnej;
12) weryfikację komunikacji w lokalizacji podstawowej;
13) weryfikację komunikacji w lokalizacji zapasowej;
14) weryfikację komunikacji pomiędzy lokalizacjami;
15) weryfikację segmentacji i separacji ruchu;
16) weryfikację działania usług systemu RIS uruchamianych w środowisku;
17) weryfikację wysokiej dostępności;
18) weryfikację działania po awarii pojedynczego hosta;
19) weryfikację działania po awarii pojedynczego urządzenia aktywnego;
20) weryfikację działania po awarii pojedynczej ścieżki komunikacyjnej;
21) weryfikację działania po utracie połączenia między lokalizacjami;
22) weryfikację backupu;
23) weryfikację odtwarzania danych;
24) weryfikację replikacji;
25) weryfikację przełączenia do lokalizacji zapasowej;
26) weryfikację powrotu do lokalizacji podstawowej;
27) weryfikację monitoringu technicznego;
28) weryfikację alarmowania;
29) weryfikację logowania zdarzeń;
30) weryfikację bezpieczeństwa dostępu administracyjnego;
31) weryfikację aktualności dokumentacji;
32) weryfikację przekazania poświadczeń i konfiguracji Zamawiającemu;
33) weryfikację zgodności z wymaganiami BCP i DRP;
34) weryfikację możliwości eksploatacji środowiska przez administratorów Zamawiającego.

Warunkiem odbioru środowiska pracy zmodernizowanego systemu RIS jest potwierdzenie, że środowisko zostało zaprojektowane, dostarczone, zamontowane, skonfigurowane, zabezpieczone, zintegrowane, przetestowane, udokumentowane i przekazane do eksploatacji zgodnie z wymaganiami PFU, dokumentacją projektową oraz wymaganiami Zamawiającego.

Odbiór nie może nastąpić w przypadku występowania nieusuniętych wad krytycznych lub istotnych, które wpływają na bezpieczeństwo, dostępność, możliwość odtworzenia, integralność danych, funkcjonowanie usług systemu RIS, komunikację pomiędzy lokalizacjami, backup, replikację, monitoring albo możliwość eksploatacji środowiska przez Zamawiającego.

1.2.14.16. Szkolenie, przekazanie wiedzy i eksploatacja

Generalny Wykonawca zobowiązany jest zapewnić przekazanie wiedzy administratorom i służbom technicznym Zamawiającego w zakresie eksploatacji środowiska pracy zmodernizowanego systemu RIS.

Zakres przekazania wiedzy musi obejmować co najmniej:

1) architekturę środowiska;
2) lokalizację podstawową i zapasową;
3) zasady działania warstwy obliczeniowej;
4) zasady działania wirtualizacji;
5) zasady działania pamięci masowej;
6) zasady działania LAN;
7) zasady działania SAN albo warstwy równoważnej;
8) backup;
9) replikację;
10) odtwarzanie po awarii;
11) monitoring;
12) alarmowanie;
13) bezpieczeństwo;
14) administrację kontami;
15) wykonywanie zmian;
16) aktualizacje;
17) procedury serwisowe;
18) procedury awaryjne;
19) odczytywanie dokumentacji;
20) sposób zgłaszania i obsługi problemów.

W okresie gwarancji Generalny Wykonawca zobowiązany jest utrzymywać środowisko pracy systemu RIS w stanie zgodnym z wymaganiami PFU, usuwać wady, wspierać Zamawiającego w diagnostyce, analizować zdarzenia, aktualizować dokumentację po zmianach oraz wykonywać czynności serwisowe i utrzymaniowe zgodnie z umową, gwarancją, dokumentacją eksploatacyjną oraz Szczegółowym Planem Przeglądów i Aktualizacji.

1.2.14.17. Rezultat końcowy

Rezultatem realizacji wymagań określonych w niniejszym rozdziale musi być kompletne, dwulokalizacyjne środowisko pracy zmodernizowanego systemu RIS, gotowe do uruchomienia produkcyjnego i eksploatacji przez Zamawiającego.

Środowisko musi zapewniać warunki techniczne do pracy usług systemu RIS, replikacji danych, wykonywania kopii zapasowych, odtwarzania po awarii, monitorowania, zarządzania, zabezpieczenia, aktualizacji, utrzymania i dalszej rozbudowy.

Generalny Wykonawca odpowiada za kompletność rozwiązania, prawidłowość doboru komponentów, zgodność z wymaganiami PFU, integrację z zasobami Zamawiającego, integrację z lokalizacją zapasową i łączem między lokalizacjami, poprawność dokumentacji, skuteczność testów oraz przekazanie środowiska do eksploatacji.

1.2.15. Wymagania dla usług cyfrowych

1.2.15.1. Przedmiot i cel wymagań

Przedmiotem niniejszego rozdziału jest określenie wymagań Zamawiającego dotyczących zaprojektowania, dostarczenia, wdrożenia, skonfigurowania, zintegrowania, uruchomienia, przetestowania i przekazania do eksploatacji usług cyfrowych systemu RIS objętych przedmiotem zamówienia.

Usługi cyfrowe RIS muszą wspierać realizację zadań Centrum RIS, w szczególności w zakresie śledzenia i namierzania jednostek, budowania strategicznego obrazu ruchu, obsługi danych AIS, prezentacji informacji na mapie operatorskiej, analizy ruchu jednostek, obsługi danych historycznych, generowania alertów, raportowania, integracji z urządzeniami i podsystemami RIS oraz udostępniania danych innym komponentom systemu RIS.

Generalny Wykonawca zobowiązany jest dostarczyć rozwiązanie kompletne, zintegrowane, bezpieczne, skalowalne, udokumentowane, możliwe do utrzymania, dalszego rozwoju oraz eksploatacji przez Zamawiającego po zakończeniu realizacji przedmiotu zamówienia.

Usługi cyfrowe muszą być zgodne z wymaganiami dotyczącymi RIS, Inland ECDIS, Inland AIS, VTT, cyberbezpieczeństwa, dostępności cyfrowej, interoperacyjności, jakości danych, monitoringu technicznego, dokumentacji, testów, odbiorów, gwarancji i utrzymania określonymi w PFU, dokumentach branżowych, Umowie oraz obowiązujących przepisach prawa, normach i standardach.

1.2.15.2. Zakres usług cyfrowych objętych zamówieniem

Zakres usług cyfrowych objętych niniejszym zamówieniem obejmuje co najmniej:

1) dostawę albo wykonanie systemu VTT, rozumianego jako usługa śledzenia i namierzania jednostek oraz budowania operatorskiego obrazu ruchu jednostek na obszarze działania systemu RIS;

2) integrację systemu VTT z urządzeniami i podsystemami systemu RIS, w szczególności ze stacjami bazowymi AIS, systemem transmisji danych, systemem CCTV w zakresie generowania raportów statystycznych, danymi hydrologicznymi, danymi meteorologicznymi, monitoringiem technicznym oraz środowiskiem pracy systemu RIS;
3) obsługę elektronicznych map nawigacyjnych Inland ENC oraz warstw mapowych niezbędnych do pracy operatorów Centrum RIS;
4) obsługę aktualnego ruchu jednostek na mapie w oparciu o dane Inland AIS;
5) obsługę danych historycznych ruchu jednostek;
6) mechanizmy wyszukiwania jednostek;
7) mechanizmy tworzenia wirtualnych bramek, stref, alarmów i powiadomień;
8) mechanizmy obliczania ETA;
9) narzędzia pomiarowe i analityczne;
10) mechanizmy statystyk, raportów i eksportu danych;
11) mechanizmy administracyjne, konfiguracyjne, utrzymaniowe, monitorujące i audytowe dla usług cyfrowych;
12) dokumentację, szkolenia, testy i przekazanie do eksploatacji.

System VTT dostarczany w ramach niniejszego zamówienia musi stanowić rozwiązanie produkcyjne, gotowe do pracy w środowisku Centrum RIS, zintegrowane z pozostałymi elementami systemu RIS oraz zapewniające obsługę zarówno istniejących, jak i nowych stacji bazowych AIS objętych systemem RIS.

1.2.15.3. Relacja do aplikacji mapowej i innych usług RIS

Mapa operatorska systemu VTT stanowi część usługi cyfrowej VTT i służy operatorom Centrum RIS do zobrazowania ruchu jednostek, danych AIS, danych referencyjnych, warstw mapowych, stref, bramek, alertów i informacji operacyjnych.

Wymagania dotyczące systemu VTT nie oznaczają rozszerzenia zakresu niniejszego zamówienia o odrębną aplikację mapową dla użytkowników zewnętrznych śródlądowych dróg wodnych, jeżeli aplikacja taka jest realizowana przez Zamawiającego w ramach odrębnego zamówienia. Generalny Wykonawca zobowiązany jest jednak zapewnić, aby dane, usługi, API, interfejsy i mechanizmy integracyjne dostarczane w ramach niniejszego zamówienia mogły być wykorzystywane przez inne rozwiązania Zamawiającego, w tym przez aplikację mapową, stronę internetową RIS albo inne przyszłe komponenty systemu RIS.

System VTT musi zostać zaprojektowany w sposób umożliwiający współpracę z pozostałymi usługami RIS, w szczególności z usługami informacji hydrologicznej i meteorologicznej, danymi NtS, systemem CCTV, systemem VHF/AIS/DGNSS, siecią transmisji danych, monitoringiem technicznym oraz integracjami zewnętrznymi.

1.2.15.4. Wymagania ogólne dla systemu VTT

Generalny Wykonawca zobowiązany jest dostarczyć system VTT spełniający co najmniej następujące wymagania ogólne:

1) system musi umożliwiać podgląd aktualnego ruchu jednostek na mapie w oparciu o dane Inland AIS;
2) system musi umożliwiać budowanie strategicznego obrazu ruchu jednostek w obszarze działania systemu RIS;
3) system musi umożliwiać obsługę danych ze wszystkich stacji bazowych AIS wchodzących w skład systemu RIS, w tym stacji istniejących, modernizowanych i nowych;
4) system musi umożliwiać odbiór, dekodowanie, przetwarzanie, prezentację, archiwizację i analizę komunikatów AIS;
5) system musi prezentować na mapie tylko jeden obiekt jednostki w przypadku odebrania tego samego komunikatu AIS przez więcej niż jedną stację bazową AIS;
6) system musi umożliwiać określenie, która stacja bazowa AIS odebrała dany komunikat AIS oraz kiedy nastąpił jego odbiór;
7) system musi umożliwiać pracę w trybie ciągłym;
8) system musi umożliwiać działanie procesów przetwarzania danych, alarmowania i zliczania ruchu w tle, niezależnie od faktu zalogowania operatora do interfejsu użytkownika;
9) system musi zapewniać dostęp do aktualnych i historycznych informacji przetwarzanych przez system RIS wyłącznie uprawnionym użytkownikom;
10) system musi zapewniać mechanizmy administracji, konfiguracji, uprawnień, logowania, audytu, monitorowania, raportowania i diagnostyki;
11) system musi być skalowalny i umożliwiać rozszerzenie zakresu terytorialnego, liczby stacji AIS, liczby kamer, liczby użytkowników, liczby stref, liczby bramek oraz liczby analizowanych zdarzeń;
12) system musi być dostosowany do pracy w środowisku produkcyjnym Centrum RIS;
13) system musi być wykonany jako rozwiązanie bezpieczne, utrzymywalne, udokumentowane i możliwe do dalszego rozwoju;
14) system musi umożliwiać integrację z monitoringiem technicznym zasobów infrastrukturalnych i aplikacyjnych systemu RIS.

1.2.15.5. Obsługa map Inland ENC i warstw mapowych

System VTT musi zapewniać obsługę śródlądowych elektronicznych map nawigacyjnych Inland ENC oraz ich wykorzystanie jako podstawowego podkładu mapowego dla zobrazowania ruchu jednostek.

Obsługa Inland ENC musi obejmować co najmniej:

1) wyświetlanie elektronicznej mapy nawigacyjnej w sposób odpowiadający wymaganiom pracy operatorskiej systemu RIS;
2) obsługę podstawowych warstw mapowych wymaganych do pracy operatora, w szczególności wody, lądu, nabrzeży, marin, oznakowania nawigacyjnego, kilometrażu oraz sieci infrastruktury;
3) prezentację danych mapowych w sposób czytelny, skalowalny i dostosowany do pracy na stanowiskach operatorskich;
4) możliwość zmiany skali mapy;
5) możliwość przesuwania, przybliżania i oddalania widoku mapy;
6) możliwość konfiguracji pozycji i skali początkowej widoku mapy;
7) możliwość włączania i wyłączania wybranych warstw mapowych;
8) możliwość wyszukiwania obiektów mapowych, w tym co najmniej według nazwy drogi wodnej, miejscowości, kilometrażu albo innego identyfikatora danych referencyjnych, jeżeli dane takie są dostępne;
9) możliwość prezentacji danych AIS, stref, bramek, alertów, tras historycznych, punktów pomiarowych oraz innych danych operacyjnych na podkładzie mapowym;
10) obsługę samodzielnej aktualizacji danych Inland ENC przez Zamawiającego.

Generalny Wykonawca zobowiązany jest zapewnić mechanizmy umożliwiające Zamawiającemu samodzielną aktualizację map Inland ENC, obejmujące co najmniej:

1) import nowych albo zaktualizowanych danych mapowych;
2) walidację techniczną importowanych danych;
3) kontrolę wersji danych mapowych;
4) możliwość wycofania albo zastąpienia danych mapowych;
5) rejestrację daty i osoby wykonującej aktualizację;
6) dokumentowanie procesu aktualizacji;
7) instrukcję aktualizacji map przeznaczoną dla administratorów Zamawiającego.

Zamawiający dopuszcza stosowanie warstw rastrowych jako uzupełnienia zobrazowania mapowego, pod warunkiem, że nie ograniczy to wymaganej obsługi danych Inland ENC, prezentacji danych AIS, działania funkcji operatorskich, mechanizmów wyszukiwania, tworzenia stref i bramek, analizy ruchu, raportowania oraz aktualizacji danych przez Zamawiającego.

1.2.15.6. Prezentacja aktualnego ruchu jednostek

System VTT musi umożliwiać prezentację aktualnego ruchu jednostek na mapie w oparciu o dane Inland AIS.

Prezentacja ruchu jednostek musi obejmować co najmniej:

1) automatyczne wyświetlanie jednostek znajdujących się w obszarze widoku mapy;
2) automatyczne aktualizowanie pozycji jednostek na mapie;
3) prezentację symbolu jednostki zgodnie z jej położeniem i kierunkiem ruchu;
4) prezentację etykiety jednostki, w tym co najmniej nazwy jednostki albo innego identyfikatora konfigurowanego przez użytkownika;
5) możliwość włączenia, wyłączenia i konfiguracji etykiet jednostek;
6) możliwość filtrowania jednostek według dostępnych kryteriów;
7) możliwość sortowania listy jednostek;
8) możliwość wskazania jednostki na mapie i wyświetlenia jej szczegółów;
9) możliwość przejścia z listy jednostek do lokalizacji jednostki na mapie;
10) wizualne rozróżnianie jednostek według typu, statusu albo innego kryterium dostępnego w danych AIS;
11) prezentację informacji o aktualności danych, w tym czasu ostatniego odebranego komunikatu;
12) sygnalizację utraty aktualności danych albo braku odświeżenia pozycji jednostki w zdefiniowanym czasie.

System musi obsługiwać dane ze wszystkich stacji bazowych AIS włączonych do systemu RIS oraz musi uwzględniać sytuację, w której ta sama jednostka albo ten sam komunikat zostanie odebrany przez więcej niż jedną stację bazową AIS.

1.2.15.7. Szczegółowe informacje o jednostkach

System VTT musi umożliwiać wyświetlanie szczegółowych informacji o jednostkach na podstawie danych AIS oraz danych dostępnych w systemie RIS.

Zakres prezentowanych informacji o jednostce musi obejmować co najmniej:

1) nazwę jednostki;
2) numer MMSI;
3) znak wywoławczy, jeżeli jest dostępny;
4) typ jednostki;
5) pozycję geograficzną;
6) kurs;
7) prędkość;
8) kierunek ruchu;
9) zanurzenie, jeżeli jest dostępne;

10) status nawigacyjny, jeżeli jest dostępny;
11) wymiary jednostki, jeżeli są dostępne;
12) czas ostatniego odebranego komunikatu AIS;
13) stację albo stacje bazowe AIS, które odebrały ostatni komunikat;
14) historię zmian pozycji w wymaganym okresie archiwizacji;
15) inne dane AIS dostępne w odebranych komunikatach, jeżeli są przetwarzane przez system.

System musi umożliwiać prezentację danych szczegółowych w sposób uporządkowany, czytelny i dostosowany do potrzeb pracy operatora, z możliwością grupowania informacji w logiczne sekcje.

1.2.15.8. Wyszukiwanie jednostek i obiektów

System VTT musi zapewniać funkcjonalność wyszukiwania jednostek co najmniej według:

1) nazwy jednostki;
2) numeru MMSI;
3) znaku wywoławczego.

Wyniki wyszukiwania muszą umożliwiać co najmniej:

1) przejście do pozycji jednostki na mapie;
2) wyświetlenie szczegółowych informacji o jednostce;
3) wyświetlenie historii ruchu jednostki;
4) filtrowanie wyników;
5) sortowanie wyników;
6) wskazanie czy jednostka jest aktualnie widoczna w systemie, czy występuje jedynie w danych historycznych.

System powinien umożliwiać również wyszukiwanie elementów mapy i danych referencyjnych, w szczególności nazwy drogi wodnej, miejscowości, kilometrażu, obiektów infrastruktury, mostów, nabrzeży, marin albo innych danych dostępnych w wykorzystywanych warstwach mapowych.

1.2.15.9. Historia ruchu jednostek

System VTT musi umożliwiać dostęp do historii ruchu jednostek oraz prezentację historycznej trasy jednostki na mapie.

1) Historia ruchu jednostek musi spełniać co najmniej następujące wymagania:
2) dostęp do danych historycznych co najmniej 5 dni wstecz;
3) prezentacja historycznej trasy jednostki na mapie;
4) możliwość wyboru zakresu czasu prezentowanej historii;
5) możliwość odtworzenia przebiegu trasy jednostki w zadanym przedziale czasu;
6) możliwość identyfikacji punktów historycznej trasy wraz z datą, godziną, pozycją, kursem i prędkością, jeżeli dane te są dostępne;
7) możliwość przejścia z danych historycznych do szczegółowych informacji o jednostce;
8) możliwość filtrowania danych historycznych według jednostki, czasu, strefy albo bramki;
9) możliwość wykorzystania danych historycznych w raportach i analizach ruchu.

Wymaganie dostępu do historii ruchu co najmniej 5 dni wstecz nie ogranicza obowiązku zapewnienia dłuższej retencji danych, jeżeli wynika ona z innych wymagań PFU, Umowy, dokumentacji projektowej, dokumentacji eksploatacyjnej albo uzgodnionej architektury systemu.

1.2.15.10. Integracja z urządzeniami i podsystemami RIS

System VTT musi zostać zintegrowany z urządzeniami i podsystemami systemu RIS w zakresie niezbędnym do realizacji funkcji śledzenia, namierzania, zobrazowania, alarmowania, raportowania i analizy ruchu.

Integracja musi obejmować co najmniej:

1) wszystkie stacje bazowe AIS funkcjonujące w systemie RIS;
2) nowe stacje bazowe AIS realizowane w ramach niniejszego zamówienia;
3) istniejące stacje bazowe AIS, jeżeli są wykorzystywane przez system RIS;
4) sieć transmisji danych systemu RIS;
5) środowisko pracy zmodernizowanego systemu RIS;
6) monitoring techniczny zasobów systemu RIS;
7) system CCTV w zakresie wymaganym do prezentacji, korelacji albo analizy ruchu;
8) źródła danych hydrologicznych i meteorologicznych w zakresie wymaganym do prezentacji danych operatorskich;
9) mechanizmy autoryzacji, uwierzytelniania, kontroli dostępu i logowania;
10) mechanizmy backupu, archiwizacji, odtwarzania i utrzymania.

Generalny Wykonawca zobowiązany jest zapewnić, aby system VTT poprawnie przetwarzał dane z każdej stacji bazowej AIS, umożliwiał identyfikację źródła danych, obsługiwał duplikaty komunikatów oraz zapewniał spójne zobrazowanie jednostek w aplikacji operatorskiej.

1.2.15.11. Wirtualne bramki, strefy, alarmy i powiadomienia

System VTT musi umożliwiać tworzenie, edycję, usuwanie, aktywowanie, dezaktywowanie i monitorowanie wirtualnych bramek oraz stref na mapie.

Funkcjonalność bramek i stref musi obejmować co najmniej:

1) tworzenie bramki jako linii, odcinka albo innego obiektu geometrycznego na mapie;
2) tworzenie strefy jako obszaru zamkniętego na mapie;
3) nadawanie nazwy, opisu, typu i statusu bramce albo strefie;
4) przypisanie reguł alarmowych do bramki albo strefy;
5) generowanie alarmu przekroczenia bramki;
6) generowanie alarmu wejścia jednostki do strefy;
7) generowanie alarmu wyjścia jednostki ze strefy;
8) identyfikację jednostki na podstawie danych AIS;
9) rejestrację daty i godziny zdarzenia;
10) rejestrację kierunku przekroczenia bramki, jeżeli jest to możliwe na podstawie danych;
11) prezentację alarmu w interfejsie operatora;
12) zapis alarmu w bazie danych;
13) możliwość filtrowania i przeglądania historii alarmów;
14) możliwość konfiguracji progów, zasad i warunków alarmowania;
15) możliwość powiązania bramki albo strefy z raportowaniem statystycznym ruchu jednostek.

Generowanie alarmów przekroczenia stref, wejścia do strefy, wyjścia ze strefy oraz przekroczenia bramki musi działać niezależnie od faktu zalogowania operatora do systemu. Mechanizmy alarmowe muszą działać jako procesy systemowe w tle, pracujące w sposób ciągły, o ile system i jego komponenty źródłowe pozostają dostępne.

System musi umożliwiać konfigurację alertów i powiadomień, w tym co najmniej:

1) konfigurację typów zdarzeń generujących alerty;
2) konfigurację priorytetów alertów;
3) konfigurację odbiorców albo grup odbiorców alertów;

4) konfigurację sposobu prezentacji alertów w interfejsie operatora;
5) rejestrację historii alertów;
6) potwierdzanie obsługi alertu przez operatora;
7) filtrowanie alertów według typu, czasu, jednostki, strefy, bramki albo statusu.

1.2.15.12. Narzędzia pomiarowe i funkcje ETA

System VTT musi zapewniać narzędzia wspierające pracę operatora na mapie, w tym co najmniej narzędzie do tworzenia okręgu odległości.

Narzędzie okręgu odległości musi umożliwiać co najmniej:

1) wskazanie punktu centralnego na mapie;
2) określenie promienia okręgu;
3) prezentację okręgu na mapie;
4) zmianę promienia albo położenia okręgu;
5) wykorzystanie okręgu jako pomocniczego narzędzia analitycznego podczas obserwacji ruchu jednostek.

System VTT musi posiadać funkcjonalność przeliczania ETA. Funkcjonalność ta musi umożliwiać co najmniej:

1) wskazanie jednostki, dla której obliczane jest ETA;
2) wskazanie punktu, bramki, strefy, kilometrażu albo obiektu docelowego;
3) obliczenie przewidywanego czasu dotarcia na podstawie dostępnych danych o pozycji, prędkości i trasie;
4) aktualizację ETA w przypadku zmiany danych wejściowych;
5) prezentację wyniku obliczenia w interfejsie operatora;
6) wykorzystanie ETA w analizach, alertach albo raportach, jeżeli zostanie to przewidziane w dokumentacji projektowej.

Generalny Wykonawca zobowiązany jest opisać w dokumentacji projektowej algorytm, założenia i ograniczenia funkcjonalności ETA, w szczególności sposób uwzględniania danych AIS, prędkości jednostki, geometrii drogi wodnej, punktów odniesienia, bramek, stref i kilometrażu.

1.2.15.13. Statystyki ruchu jednostek i raportowanie

System VTT musi zapewniać obsługę statystyk ruchu jednostek na bazie danych ze stacji AIS oraz kamer obserwacyjnych ulokowanych na granicach strefy RIS.

Statystyki ruchu jednostek muszą obejmować:

1) jednostki wyposażone w transpondery pokładowe AIS, identyfikowane na podstawie danych AIS;
2) jednostki niewyposażone w transpondery pokładowe AIS, identyfikowane albo zliczane na podstawie danych z kamer obserwacyjnych ulokowanych na granicach strefy RIS, w zakresie wynikającym z możliwości technicznych systemu CCTV, przyjętej architektury analizy obrazu oraz jakości danych wideo.

System musi umożliwiać co najmniej:

1) automatyczne zliczanie jednostek w określonych strefach;
2) zliczanie przekroczeń zdefiniowanych bramek;
3) zliczanie wejść do strefy;
4) zliczanie wyjść ze strefy;
5) zliczanie jednostek według przedziału czasu;
6) zliczanie jednostek według kierunku ruchu, jeżeli jest to możliwe na podstawie danych;
7) zliczanie jednostek według typu, jeżeli typ jest dostępny w danych AIS albo możliwy do określenia na podstawie przyjętych reguł;
8) rozróżnienie statystyk opartych na danych AIS i statystyk opartych na danych z kamer;
9) ręczną korektę albo oznaczenie zdarzeń wątpliwych, jeżeli automatyczna klasyfikacja nie jest możliwa;
10) prezentację danych statystycznych w interfejsie użytkownika;
11) generowanie raportów dziennych;
12) generowanie raportów miesięcznych;
13) generowanie raportów rocznych;
14) generowanie raportów dla wskazanej strefy, bramki, lokalizacji, odcinka drogi wodnej albo zakresu czasu;
15) eksport raportów do formatu PDF;
16) eksport raportów do formatu XLS albo XLSX;
17) zachowanie historii wygenerowanych raportów albo możliwość ich ponownego wygenerowania na podstawie danych źródłowych.

Generalny Wykonawca zobowiązany jest w dokumentacji projektowej opisać metodykę zliczania jednostek, zasady eliminacji duplikatów, zasady korelacji danych AIS i CCTV, sposób identyfikacji jednostek nieposiadających AIS, ograniczenia dokładności zliczania oraz sposób raportowania zdarzeń niejednoznacznych.

Jeżeli pełna automatyczna identyfikacja jednostek niewyposażonych w transponder AIS nie jest możliwa na podstawie dostępnych danych z kamer, system musi co najmniej umożliwiać automatyczne albo półautomatyczne zliczanie takich jednostek w zdefiniowanych punktach obserwacyjnych oraz oznaczanie źródła i poziomu wiarygodności danych.

1.2.15.14. Interfejs użytkownika

System VTT musi posiadać nowoczesny, intuicyjny, czytelny i ergonomiczny interfejs użytkownika dostosowany do pracy operatorów Centrum RIS.

Interfejs użytkownika musi spełniać co najmniej następujące wymagania:

1) zapewniać dostęp do podstawowych funkcji VTT z poziomu logicznie uporządkowanych widoków;
2) umożliwiać pracę na mapie operatorskiej;
3) umożliwiać jednoczesną obsługę mapy, listy jednostek, szczegółów jednostki, alertów, stref, bramek i raportów;
4) umożliwiać filtrowanie i sortowanie danych;
5) prezentować informacje o aktualnie zalogowanym użytkowniku;
6) prezentować czas ostatniej aktualizacji danych;
7) zapewniać możliwość konfiguracji wybranych preferencji użytkownika;
8) ograniczać dostęp do funkcji i danych zgodnie z uprawnieniami użytkownika;
9) nie prezentować użytkownikowi pól danych, funkcji albo operacji, do których użytkownik nie posiada uprawnień;
10) umożliwiać przeglądanie, eksport albo drukowanie danych i raportów w zakresie zgodnym z uprawnieniami;
11) zapewniać czytelne komunikaty błędów, ostrzeżeń, alarmów i potwierdzeń operacji;
12) być dostępny w języku polskim;
13) spełniać wymagania dostępności cyfrowej określone w PFU, w zakresie właściwym dla danej klasy interfejsu i jego użytkowników.

Generalny Wykonawca zobowiązany jest przedstawić Zamawiającemu do akceptacji projekt interfejsu użytkownika, obejmujący co najmniej główne widoki systemu, widok mapy, widok listy jednostek, widok szczegółów jednostki, widok historii trasy, widok stref i bramek, widok alarmów, widok raportów oraz widoki administracyjne.

1.2.15.15. Administracja, role i uprawnienia

System VTT oraz pozostałe usługi cyfrowe muszą posiadać mechanizmy administracyjne umożliwiające bezpieczne zarządzanie użytkownikami, rolami, uprawnieniami, konfiguracją, słownikami, parametrami pracy, strefami, bramkami, alertami i raportami.

Mechanizmy administracyjne muszą umożliwiać co najmniej:

1) tworzenie, edycję, blokowanie i usuwanie kont użytkowników, jeżeli system posiada własny mechanizm kont;
2) integrację z mechanizmami uwierzytelniania Zamawiającego, jeżeli zostanie to przewidziane w dokumentacji projektowej;
3) przypisywanie użytkowników do ról;
4) definiowanie uprawnień do funkcji, danych, raportów, konfiguracji i administracji;
5) rejestrowanie działań administracyjnych;
6) konfigurację źródeł danych;
7) konfigurację stacji AIS;
8) konfigurację map i warstw;
9) konfigurację stref i bramek;
10) konfigurację alertów i powiadomień;
11) konfigurację parametrów raportowania;
12) eksport i import konfiguracji;
13) wykonanie kopii konfiguracji;
14) odtworzenie konfiguracji po awarii.

1.2.15.16. Dane, archiwizacja i jakość danych

System VTT musi zapewniać przetwarzanie danych w sposób spójny, audytowalny i umożliwiający późniejszą analizę, raportowanie oraz odtworzenie przebiegu zdarzeń.

Generalny Wykonawca zobowiązany jest zapewnić co najmniej:

1) zapis danych AIS niezbędnych do prezentacji aktualnego ruchu;
2) zapis danych AIS niezbędnych do odtworzenia historii ruchu co najmniej 5 dni wstecz;
3) zapis zdarzeń stref, bramek, alarmów i alertów;
4) zapis wyników zliczania jednostek i danych statystycznych;
5) zapis informacji o źródle danych, w tym stacji AIS albo kamery;
6) znaczniki czasu dla danych i zdarzeń;
7) mechanizmy eliminacji duplikatów komunikatów AIS;
8) mechanizmy oznaczania danych nieaktualnych, niekompletnych albo niespójnych;

9) mechanizmy kontroli jakości danych w zakresie właściwym dla danych AIS, danych mapowych, danych CCTV oraz danych statystycznych;
10) możliwość backupu i odtworzenia danych zgodnie z wymaganiami dotyczącymi środowiska pracy systemu RIS.

Generalny Wykonawca zobowiązany jest opisać w dokumentacji projektowej model danych systemu VTT, zakres danych archiwizowanych, retencję danych, zasady indeksowania danych, zasady agregacji statystyk, zasady usuwania danych, zasady odtwarzania danych oraz zależności z systemem backupu i replikacji.

1.2.15.17. Wydajność, skalowalność i niezawodność

System VTT i pozostałe usługi cyfrowe muszą zostać zaprojektowane i wykonane z uwzględnieniem wymagań wydajnościowych, skalowalności i niezawodności właściwych dla pracy Centrum RIS.

Generalny Wykonawca zobowiązany jest zapewnić co najmniej:

1) obsługę wszystkich stacji bazowych AIS wchodzących w skład systemu RIS;
2) obsługę zakładanego wolumenu komunikatów AIS;
3) obsługę równoczesnej pracy wielu operatorów;
4) obsługę wymaganej liczby stref, bramek i reguł alarmowych;
5) obsługę raportowania dziennego, miesięcznego i rocznego;
6) działanie procesów alarmowych i zliczających w tle;
7) odporność na krótkotrwałe zaniki danych źródłowych;
8) mechanizmy ponawiania przetwarzania danych po przerwie;
9) monitoring działania usług aplikacyjnych;
10) możliwość rozbudowy systemu o kolejne lokalizacje, stacje, warstwy danych, użytkowników i raporty.

Wymagania dotyczące szczegółowych parametrów wydajności, dostępności i SLA, jeżeli nie zostały określone w PFU, zostaną określone w Umowie albo dokumentacji projektowej zaakceptowanej przez Zamawiającego.

1.2.15.18. Cyberbezpieczeństwo i ochrona dostępu

System VTT oraz pozostałe usługi cyfrowe muszą spełniać wymagania cyberbezpieczeństwa określone w PFU oraz Umowie.

Generalny Wykonawca zobowiązany jest zapewnić co najmniej:

1) uwierzytelnianie użytkowników;
2) autoryzację dostępu do funkcji i danych;
3) rozdzielenie ról operatorskich, administracyjnych, serwisowych i odczytowych;
4) rejestrowanie działań użytkowników i administratorów;
5) ochronę danych przesyłanych pomiędzy komponentami systemu;
6) ochronę interfejsów administracyjnych;
7) bezpieczne zarządzanie kontami technicznymi;
8) brak wykorzystywania domyślnych haseł po przekazaniu systemu do eksploatacji;
9) możliwość zmiany haseł, kluczy, certyfikatów i innych danych uwierzytelniających;
10) mechanizmy aktualizacji oprogramowania i usuwania podatności;
11) ochronę przed nieuprawnionym dostępem do danych AIS, raportów, konfiguracji, map, stref i bramek;
12) zgodność z wymaganiami logowania, monitorowania i reagowania na incydenty określonymi w PFU.

1.2.15.19. Monitoring techniczny usług cyfrowych

Usługi cyfrowe, w tym system VTT, muszą zostać objęte monitoringiem technicznym zasobów infrastrukturalnych i aplikacyjnych systemu RIS.

Monitoring musi obejmować co najmniej:

1) dostępność aplikacji VTT;
2) dostępność usług backendowych;
3) dostępność bazy danych albo baz danych wykorzystywanych przez system VTT;
4) dostępność źródeł danych AIS;
5) dostępność integracji ze stacjami bazowymi AIS;
6) dostępność integracji z CCTV, jeżeli jest wykorzystywana przez system VTT;
7) dostępność integracji z danymi hydrologicznymi i meteorologicznymi;
8) poprawność działania procesów przetwarzania danych AIS;
9) poprawność działania procesów alarmowych;
10) poprawność działania procesów statystycznych i raportowych;
11) liczbę odebranych komunikatów AIS albo inne miary przepływu danych;
12) błędy importu albo aktualizacji map;
13) wykorzystanie zasobów systemowych;
14) zdarzenia krytyczne, ostrzegawcze i informacyjne.

System musi generować alarmy techniczne w przypadku niedostępności usług, utraty danych ze stacji AIS, opóźnień przetwarzania, błędów procesów alarmowych, błędów raportowania, błędów integracji, przekroczenia progów zasobów albo innych zdarzeń mogących wpływać na prawidłową pracę operatorów Centrum RIS.

1.2.15.20. Dokumentacja

Generalny Wykonawca zobowiązany jest opracować i przekazać Zamawiającemu kompletną dokumentację usług cyfrowych, w tym systemu VTT.

Dokumentacja musi obejmować co najmniej:

1) dokumentację projektową;
2) opis architektury systemu;
3) model danych;
4) opis źródeł danych;
5) opis integracji;
6) opis obsługi danych Inland ENC i procedury ich aktualizacji;
7) opis konfiguracji stacji AIS;
8) opis konfiguracji map, warstw, stref i bramek;
9) opis mechanizmów alarmowych i powiadomień;
10) opis funkcjonalności ETA;
11) opis metodyki statystyk ruchu jednostek;
12) opis korelacji danych AIS i CCTV;
13) dokumentację administratora;
14) dokumentację operatora;
15) dokumentację utrzymaniową;
16) dokumentację bezpieczeństwa;
17) dokumentację API i interfejsów, jeżeli są dostarczane;
18) procedury backupu i odtwarzania;
19) procedury aktualizacji systemu;
20) procedury aktualizacji map Inland ENC;
21) procedury obsługi awarii;
22) dokumentację testową i odbiorową;
23) dokumentację powykonawczą.

Dokumentacja musi zostać sporządzona w języku polskim, z wyjątkiem kart katalogowych, dokumentacji producentów i dokumentacji technicznej standardowych komponentów, które mogą zostać przekazane w języku polskim albo angielskim, jeżeli producent nie udostępnia wersji polskiej.

1.2.15.21. Szkolenia i przekazanie wiedzy

Generalny Wykonawca zobowiązany jest przeprowadzić szkolenia dla operatorów, administratorów i personelu technicznego Zamawiającego w zakresie dostarczonych usług cyfrowych.

Szkolenia muszą obejmować co najmniej:

1) architekturę systemu VTT;
2) obsługę interfejsu operatora;
3) pracę z mapą operatorską i warstwami Inland ENC;
4) obsługę aktualnego ruchu jednostek;
5) wyszukiwanie jednostek;
6) obsługę szczegółowych informacji o jednostkach;
7) obsługę historii ruchu i past track;
8) tworzenie, edycję i obsługę stref oraz bramek;
9) obsługę alarmów i powiadomień;
10) korzystanie z narzędzia okręgu odległości;
11) korzystanie z funkcjonalności ETA;
12) generowanie raportów i statystyk;
13) eksport raportów do PDF i XLS albo XLSX;
14) administrację użytkownikami, rolami i uprawnieniami;
15) aktualizację map Inland ENC;
16) podstawową diagnostykę problemów;
17) obsługę awarii i procedury odtworzeniowe;
18) zasady bezpieczeństwa i ochrony dostępu;
19) korzystanie z dokumentacji administratora i operatora.

Szkolenia muszą obejmować część teoretyczną i praktyczną oraz muszą zostać udokumentowane zgodnie z wymaganiami PFU.

1.2.15.22. Testy i odbiór usług cyfrowych

Generalny Wykonawca zobowiązany jest opracować i uzgodnić z Zamawiającym plan testów usług cyfrowych, obejmujący co najmniej system VTT, integrację z AIS, obsługę map, historię ruchu, strefy, bramki, alerty, raporty, statystyki, integrację z CCTV, monitoring techniczny, bezpieczeństwo i dokumentację.

Testy odbiorowe systemu VTT muszą obejmować co najmniej:

1) weryfikację uruchomienia systemu VTT w środowisku docelowym;
2) weryfikację obsługi wszystkich stacji bazowych AIS;
3) weryfikację odbioru i prezentacji danych AIS;
4) weryfikację eliminacji duplikatów komunikatów AIS odbieranych przez więcej niż jedną stację;
5) weryfikację identyfikacji stacji AIS, która odebrała komunikat;
6) weryfikację prezentacji jednostek na mapie;
7) weryfikację obsługi Inland ENC;
8) weryfikację procedury aktualizacji Inland ENC przez Zamawiającego;
9) weryfikację podstawowych warstw mapowych;
10) weryfikację wyszukiwania jednostek po nazwie, MMSI i znaku wywoławczym;
11) weryfikację prezentacji szczegółowych informacji o jednostce;
12) weryfikację historii ruchu co najmniej 5 dni wstecz;
13) weryfikację tworzenia i działania bramek;
14) weryfikację tworzenia i działania stref;
15) weryfikację generowania alarmu przekroczenia bramki;
16) weryfikację generowania alarmu wejścia do strefy;
17) weryfikację generowania alarmu wyjścia ze strefy;
18) weryfikację działania alarmów niezależnie od zalogowania operatora;
19) weryfikację konfiguracji alertów i powiadomień;
20) weryfikację narzędzia okręgu odległości;
21) weryfikację funkcjonalności ETA;
22) weryfikację statystyk ruchu jednostek na podstawie danych AIS;
23) weryfikację statystyk albo zliczania jednostek na podstawie kamer obserwacyjnych w zakresie przewidzianym w dokumentacji projektowej;
24) weryfikację raportów dziennych, miesięcznych i rocznych;
25) weryfikację eksportu raportów do PDF;
26) weryfikację eksportu raportów do XLS albo XLSX;

27) weryfikację uprawnień i kontroli dostępu;
28) weryfikację logowania i audytu;
29) weryfikację monitoringu technicznego usług cyfrowych;
30) weryfikację backupu i odtwarzania konfiguracji;
31) weryfikację kompletności dokumentacji;
32) weryfikację przeprowadzenia szkoleń.

Pozytywny wynik testów musi zostać potwierdzony protokołami testów i odbioru podpisanymi przez Strony.

1.2.15.23. Rezultat końcowy

Rezultatem końcowym realizacji wymagań określonych w niniejszym rozdziale musi być kompletne, uruchomione, zintegrowane, przetestowane i przekazane do eksploatacji środowisko usług cyfrowych RIS, obejmujące co najmniej system VTT umożliwiający operatorom Centrum RIS śledzenie i namierzanie jednostek, pracę na mapie operatorskiej Inland ENC, podgląd aktualnego ruchu jednostek na podstawie danych AIS, analizę historii ruchu, wyszukiwanie jednostek, obsługę stref i bramek, generowanie alarmów i powiadomień, wyliczanie ETA, prowadzenie statystyk ruchu jednostek oraz generowanie raportów.

System musi wspierać pracę Centrum RIS na całym obszarze objętym systemem RIS, obsługiwać wszystkie stacje bazowe AIS, współpracować z pozostałymi komponentami RIS oraz zapewniać możliwość dalszej rozbudowy, utrzymania i integracji z przyszłymi rozwiązaniami Zamawiającego.

1.2.16. Wymagania interoperacyjności, danych i integracji z systemami zewnętrznymi

Rozdział określa wymagania Zamawiającego dotyczące interoperacyjności, modelu danych, jakości danych, wymiany danych, integracji z systemami zewnętrznymi oraz udostępniania danych dziedzinowych przez zmodernizowany system RIS.

System RIS rozwijany w ramach projektu musi być projektowany jako element krajowego i europejskiego ekosystemu usług informacji rzecznej, a jednocześnie jako źródłowy system dziedzinowy Zamawiającego umożliwiający pozyskiwanie, przetwarzanie, prezentację, archiwizację i udostępnianie danych właściwych dla realizacji zadań RIS na Odrzańskiej Drodze Wodnej.

Wymagania określone w niniejszym rozdziale nie ograniczają się wyłącznie do integracji z systemem EuRIS. Integracja z EuRIS stanowi jedną z usług integracyjnych realizowanych przez zmodernizowany system RIS. System musi również umożliwiać realizację integracji z innymi systemami teleinformatycznymi, w szczególności z Systemem Hydrologii IMGW-PIB,

systemami własnymi Zamawiającego oraz systemami teleinformatycznymi innych instytucji uprawnionych do korzystania z danych systemu RIS.

Celem wymagań określonych w niniejszym rozdziale jest zapewnienie, aby dane dziedzinowe gromadzone i przetwarzane w systemie RIS mogły być wykorzystywane nie tylko w aplikacjach operatorskich Centrum RIS, ale również w usługach cyfrowych Zamawiającego, usługach informacyjnych dla użytkowników śródlądowych dróg wodnych, systemach administracji publicznej, systemach instytucji współpracujących oraz systemach europejskich właściwych dla usług RIS.

W ramach realizacji zamówienia Generalny Wykonawca zobowiązany jest zaprojektować, wykonać, udokumentować, uruchomić, przetestować i przekazać do eksploatacji mechanizmy wymiany danych i integracji systemu RIS, obejmujące co najmniej:

1) model danych systemu RIS;
2) zasady identyfikacji, walidacji, aktualizacji i kontroli jakości danych;
3) usługę przekazywania danych do systemu EuRIS;
4) usługę przekazywania danych z wodowskazów systemu RIS do Systemu Hydrologii IMGW-PIB;
5) udokumentowane API systemu RIS umożliwiające pobieranie danych dziedzinowych;
6) mechanizmy bezpieczeństwa, monitoringu, logowania, wersjonowania i obsługi błędów integracji;
7) dokumentację techniczną, eksploatacyjną i testową interfejsów integracyjnych.

Wymagania interoperacyjności, danych i integracji należy stosować łącznie z wymaganiami dotyczącymi systemu łączności radiowej VHF/AIS/DGNSS, systemu monitoringu wizyjnego CCTV, czujników hydrologicznych, sensorów meteorologicznych, sieci transmisji danych, usług cyfrowych RIS, cyberbezpieczeństwa, dokumentacji, testów, odbiorów, gwarancji, utrzymania oraz dalszej rozbudowy systemu RIS.

1.2.16.1. Wymagania ogólne

Generalny Wykonawca zobowiązany jest zapewnić interoperacyjność zmodernizowanego systemu RIS w wymiarze technicznym, semantycznym, organizacyjnym i prawnym.

Interoperacyjność techniczna oznacza zdolność systemu RIS do wymiany danych z innymi systemami teleinformatycznymi przy użyciu udokumentowanych interfejsów, struktur danych, protokołów komunikacyjnych, formatów wymiany danych, mechanizmów bezpieczeństwa oraz mechanizmów monitorowania i obsługi błędów.

Interoperacyjność semantyczna oznacza stosowanie jednoznacznych definicji danych, słowników, identyfikatorów, kodów, klasyfikacji, jednostek miar, statusów danych, statusów jakości, oznaczeń źródeł danych oraz reguł interpretacji danych, tak aby dane udostępniane przez system RIS mogły być poprawnie rozumiane i przetwarzane przez systemy zewnętrzne.

Interoperacyjność organizacyjna oznacza zapewnienie spójności procesów pozyskiwania, zatwierdzania, aktualizacji, korekty, publikacji, udostępniania, archiwizacji i wycofywania danych, z określeniem ról, odpowiedzialności, procedur oraz sposobów postępowania w przypadku błędów, awarii albo niezgodności danych.

Interoperacyjność prawna oznacza zapewnienie, że wymiana danych i integracja systemu RIS z systemami zewnętrznymi odbywa się zgodnie z obowiązującymi przepisami prawa, wymaganiami dotyczącymi usług informacji rzecznej, cyberbezpieczeństwa, ochrony danych, dostępności, ponownego wykorzystywania informacji, praw własności intelektualnej oraz zasadami udostępniania danych przez podmioty publiczne.

System RIS musi umożliwiać wymianę danych z systemami zewnętrznymi w sposób bezpieczny, kontrolowany, monitorowany i możliwy do audytu. W szczególności wymagane jest zapewnienie mechanizmów uwierzytelniania, autoryzacji, szyfrowania transmisji, rejestrowania zdarzeń, kontroli dostępu, monitorowania dostępności interfejsów, monitorowania skuteczności przekazywania danych oraz raportowania błędów integracyjnych.

Wymiana danych z systemami zewnętrznymi musi być realizowana w sposób zapewniający integralność, kompletność, aktualność, identyfikowalność i rozliczalność danych. System musi umożliwiać ustalenie źródła danych, czasu pozyskania danych, czasu ich przetworzenia, czasu udostępnienia, statusu jakości danych, historii zmian oraz informacji o ewentualnej korekcie danych.

Generalny Wykonawca zobowiązany jest zapewnić, aby zmodernizowany system RIS mógł udostępniać dane dziedzinowe co najmniej dla następujących kategorii danych, o ile są one gromadzone albo przetwarzane w systemie RIS:

1) dane AIS i dane wykorzystywane w usługach VTT;
2) dane hydrologiczne z wodowskazów systemu RIS;
3) dane meteorologiczne z sensorów meteorologicznych systemu RIS;
4) dane dotyczące lokalizacji, obiektów, urządzeń, sensorów, kamer i punktów pomiarowych;
5) dane przestrzenne i referencyjne dotyczące Odrzańskiej Drogi Wodnej;
6) dane dotyczące komunikatów dla kierowników statków;
7) metadane kamer CCTV i ich powiązania lokalizacyjne;
8) dane diagnostyczne, eksploatacyjne i statusowe urządzeń terenowych, w zakresie wymaganym przez Zamawiającego;
9) dane publikowane w aplikacjach, portalach, usługach mapowych albo innych usługach cyfrowych systemu RIS;
10) inne dane dziedzinowe wskazane przez Zamawiającego na etapie analizy przedwdrożeniowej, projektowania albo uzgodnień integracyjnych.

System RIS musi być przygotowany do współpracy z systemami zewnętrznymi obecnie wskazanymi w PFU oraz z systemami, które mogą zostać wskazane przez Zamawiającego w toku realizacji zamówienia, o ile ich integracja mieści się w zakresie przedmiotu zamówienia

albo wynika z wymagań prawnych, standardów RIS, uzgodnień międzyinstytucjonalnych albo potrzeb realizacji usług cyfrowych systemu RIS.

1.2.16.2. Model danych, jakość danych i słowniki referencyjne

Generalny Wykonawca zobowiązany jest opracować model danych systemu RIS obejmujący dane pozyskiwane, przetwarzane, prezentowane, przechowywane i udostępniane przez zmodernizowany system RIS.

Model danych musi obejmować co najmniej:

1) wykaz kategorii danych przetwarzanych w systemie RIS;
2) opis źródeł danych, w tym urządzeń terenowych, sensorów, systemów centralnych, komponentów aplikacyjnych, systemów zewnętrznych oraz danych wprowadzanych przez użytkowników;
3) opis struktur danych, typów danych, atrybutów, jednostek miar, słowników, kodów, klasyfikacji, statusów danych i statusów jakości;
4) opis identyfikatorów lokalizacji, obiektów, urządzeń, sensorów, kamer, stacji, punktów pomiarowych, odcinków drogi wodnej, komunikatów, zdarzeń i innych encji systemu RIS;
5) opis powiązania danych z lokalizacją przestrzenną, kilometrażem drogi wodnej, obiektem infrastruktury, punktem pomiarowym albo innym odniesieniem właściwym dla usług RIS;
6) opis reguł walidacji danych;
7) opis reguł korekty danych;
8) opis reguł agregacji, uśredniania albo przeliczania danych, jeżeli mają zastosowanie;
9) opis zasad wersjonowania, aktualizacji, archiwizacji i wycofywania danych;
10) opis zasad mapowania danych do formatów i struktur wymaganych przez systemy zewnętrzne;
11) opis zasad eksportu danych i migracji danych;
12) opis zasad kontroli jakości danych.

Model danych musi obejmować dane źródłowe oraz dane przetworzone. W szczególności dla danych pomiarowych wymagane jest rozróżnienie danych surowych, danych zwalidowanych, danych skorygowanych, danych zagregowanych i danych udostępnionych do publikacji albo do systemów zewnętrznych.

Dane pomiarowe muszą być oznaczane co najmniej identyfikatorem lokalizacji, identyfikatorem urządzenia albo punktu pomiarowego, czasem wykonania pomiaru, czasem przekazania danych do systemu RIS, wartością pomiaru, jednostką miary, statusem jakości, statusem źródła danych oraz informacją o ewentualnej korekcie albo opóźnionym przekazaniu danych.

W przypadku danych buforowanych lokalnie w czasie utraty połączenia transmisyjnego system musi zachować rzeczywisty czas wykonania pomiaru oraz umożliwiać odróżnienie danych bieżących od danych przekazanych do systemu RIS po wznowieniu transmisji.

System RIS musi zapewniać mechanizmy walidacji danych. Walidacja musi obejmować co najmniej:

1) poprawność techniczną formatu danych;
2) kompletność wymaganych pól;
3) poprawność typów danych;
4) zgodność wartości z dopuszczalnymi zakresami;
5) zgodność jednostek miar;
6) poprawność identyfikatorów lokalizacji, urządzeń, punktów pomiarowych i obiektów;
7) poprawność odniesień przestrzennych;
8) poprawność czasu pomiaru albo zdarzenia;
9) zgodność ze słownikami referencyjnymi;
10) wykrywanie danych brakujących, opóźnionych, zdublowanych, niespójnych albo przekraczających zdefiniowane progi jakości.

System musi umożliwiać zarządzanie słownikami, kodami, klasyfikacjami i danymi referencyjnymi wykorzystywanymi w usługach RIS oraz w integracjach zewnętrznych. Wymaga się zapewnienia mechanizmów wersjonowania słowników, kontroli zmian, dokumentowania źródła słownika, walidacji użycia kodów oraz aktualizacji słowników zgodnie z wymaganiami Zamawiającego i właściwych standardów.

Dane przestrzenne wykorzystywane w systemie RIS muszą być spójne z państwowym systemem odniesień przestrzennych, kilometrażem drogi wodnej, danymi mapowymi, danymi IENC, lokalizacją urządzeń terenowych oraz danymi referencyjnymi wykorzystywanymi w usługach informacji rzecznej. Wszelkie transformacje, korekty, generalizacje i przeliczenia danych przestrzennych muszą być udokumentowane.

Generalny Wykonawca zobowiązany jest zapewnić, aby model danych systemu RIS był opisany w sposób umożliwiający jego wykorzystanie przez Zamawiającego w przyszłej rozbudowie systemu, w integracjach z kolejnymi systemami zewnętrznymi, w migracji danych, w tworzeniu usług cyfrowych oraz w udostępnianiu danych innym uprawnionym podmiotom.

1.2.16.3. Usługa przekazywania danych do systemu EuRIS

Generalny Wykonawca zobowiązany jest zaprojektować, wykonać, uruchomić, udokumentować, przetestować i przekazać do eksploatacji usługę integracyjną umożliwiającą przekazywanie danych z systemu RIS do systemu EuRIS albo do innego wskazanego przez Zamawiającego punktu integracyjnego właściwego dla europejskiego ekosystemu usług informacji rzecznej.

Integracja z EuRIS musi być traktowana jako jedna z usług integracyjnych zmodernizowanego systemu RIS. Nie zwalnia ona Generalnego Wykonawcy z obowiązku zapewnienia szerszej interoperacyjności systemu RIS, opracowania modelu danych, zapewnienia jakości danych oraz wykonania udokumentowanego API systemu RIS umożliwiającego udostępnianie danych dziedzinowych Zamawiającemu i innym uprawnionym interesariuszom.

Podstawą przeprowadzenia prac analitycznych, projektowych, implementacyjnych, testowych i wdrożeniowych w zakresie integracji z EuRIS jest aktualna dokumentacja API systemu EuRIS, dokumentacja referencyjna API, dokumentacja techniczna punktów końcowych, dokumentacja encji, zasady uwierzytelniania, zasady wersjonowania, zasady paginacji, zasady limitowania zapytań, zasady obsługi błędów oraz procedury określone przez gestora, administratora albo inny właściwy podmiot odpowiedzialny za system EuRIS.

Generalny Wykonawca zobowiązany jest na etapie analizy przedwdrożeniowej zweryfikować aktualną dokumentację API systemu EuRIS, zakres dostępnych interfejsów, wymagane dane dostępowe, sposób uzyskania uprawnień, wymagane środowiska testowe, wymagane procedury dopuszczenia integracji, wymagania dotyczące publikacji danych, wymagania dotyczące oznaczania źródła danych, wymagania dotyczące jakości danych oraz wymagania dotyczące testów integracyjnych.

Generalny Wykonawca zobowiązany jest, w imieniu albo przy udziale Zamawiającego, przygotować wszystkie informacje techniczne niezbędne do uzyskania dostępu do interfejsów EuRIS, w tym informacje dotyczące podmiotu korzystającego z interfejsów, celu wykorzystania danych, wymaganych interfejsów, zakresu danych, sposobu wykorzystania danych, środowisk technicznych, bezpieczeństwa oraz osób kontaktowych. Jeżeli uzyskanie danych dostępowych, kluczy, tokenów, certyfikatów, kont technicznych albo innych mechanizmów dostępu wymaga odrębnej procedury po stronie gestora systemu EuRIS, Generalny Wykonawca zobowiązany jest uwzględnić tę procedurę w harmonogramie realizacji prac.

Zakres danych przekazywanych do EuRIS musi zostać określony na etapie analizy przedwdrożeniowej i projektowania, z uwzględnieniem wymagań Zamawiającego, właściwych standardów RIS, aktualnych wymagań technicznych EuRIS, zakresu danych dostępnych w systemie RIS oraz uzgodnień z podmiotami odpowiedzialnymi za utrzymanie albo integrację systemu EuRIS.

Usługa przekazywania danych do EuRIS musi obejmować co najmniej:

1) identyfikację danych systemu RIS wymaganych albo przewidzianych do przekazywania do EuRIS;
2) analizę aktualnej dokumentacji API EuRIS i wskazanie interfejsów, encji, endpointów, struktur danych oraz parametrów wymaganych dla integracji;
3) mapowanie danych systemu RIS do struktur, formatów, słowników, identyfikatorów i reguł wymaganych przez EuRIS;
4) walidację danych przed ich przekazaniem do EuRIS;
5) przekazywanie danych w wymaganym trybie, zakresie i częstotliwości;
6) obsługę mechanizmów uwierzytelniania i autoryzacji wymaganych przez EuRIS;

7) obsługę wersjonowania API EuRIS oraz zmian dokumentacji API w okresie realizacji zamówienia;
8) obsługę paginacji, limitów zapytań, ograniczeń technicznych, komunikatów zwrotnych i kodów błędów, jeżeli mają zastosowanie do wykorzystywanych interfejsów;
9) obsługę błędów walidacji, błędów transmisji, błędów autoryzacji, przekroczenia limitów, niedostępności usługi oraz niezgodności danych;
10) rejestrowanie zdarzeń integracyjnych;
11) monitorowanie skuteczności przekazywania danych;
12) alarmowanie o braku przekazania danych albo o błędach integracji;
13) możliwość ponownego przekazania danych, jeżeli jest to wymagane albo uzasadnione charakterem integracji;
14) dokumentację techniczną, testową, administracyjną i eksploatacyjną integracji.

W ramach integracji z EuRIS Generalny Wykonawca zobowiązany jest uwzględnić w szczególności dane referencyjne i lokalizacyjne, dane dotyczące drogi wodnej i obiektów infrastruktury, dane wykorzystywane w usługach VTT, dane AIS, komunikaty dla kierowników statków, dane hydrologiczne i meteorologiczne oraz dane przestrzenne, o ile ich przekazywanie wynika z aktualnych wymagań EuRIS, standardów RIS, dokumentacji API albo uzgodnień Zamawiającego.

System musi zapewniać możliwość kontrolowania, które dane są przekazywane do EuRIS, w jakim zakresie, z jaką częstotliwością, w jakim statusie jakości, w jakiej wersji struktury danych oraz z jakiego źródła. Zamawiający musi mieć możliwość weryfikacji poprawności danych przed ich publikacją albo przekazaniem, jeżeli taki tryb zostanie wskazany w dokumentacji projektowej, uzgodnieniach integracyjnych albo procedurach gestora systemu EuRIS.

Integracja z EuRIS musi być realizowana w sposób bezpieczny, monitorowany i możliwy do audytu. Wymaga się rejestrowania co najmniej czasu przekazania danych, zakresu przekazanych danych, wersji interfejsu, wyniku walidacji, wyniku transmisji, błędów, ponowień, komunikatów zwrotnych, statusu ostatniej skutecznej wymiany danych oraz informacji o użytkowniku technicznym albo komponencie systemowym realizującym wymianę danych.

Generalny Wykonawca zobowiązany jest zapewnić, aby integracja z EuRIS nie była realizowana poprzez ręczne, nieudokumentowane albo jednorazowe mechanizmy wymiany danych. Integracja musi mieć charakter powtarzalnej, utrzymywalnej, monitorowanej i udokumentowanej usługi integracyjnej, możliwej do dalszego utrzymania, diagnozowania i rozbudowy przez Zamawiającego albo podmioty działające na jego rzecz.

Generalny Wykonawca zobowiązany jest opracować dokumentację integracji z EuRIS obejmującą co najmniej:

1) opis celu i zakresu integracji;
2) opis podstawy formalnej i technicznej integracji;
3) wykaz wykorzystanych dokumentów API EuRIS oraz ich wersji albo daty dostępu;

4) opis wykorzystywanych interfejsów, encji i endpointów EuRIS;
5) opis mechanizmu uwierzytelniania i autoryzacji;
6) opis zakresu przekazywanych danych;
7) mapowanie danych systemu RIS do struktur wymaganych przez EuRIS;
8) opis reguł walidacji danych;
9) opis trybu i częstotliwości przekazywania danych;
10) opis obsługi paginacji, limitów, kodów błędów i komunikatów zwrotnych;
11) opis mechanizmów monitorowania i alarmowania;
12) opis mechanizmów ponawiania transmisji albo postępowania w przypadku błędów;
13) opis logowania zdarzeń integracyjnych;
14) opis procedur eksploatacyjnych;
15) opis procedur awaryjnych;
16) opis procedur aktualizacji integracji w przypadku zmiany dokumentacji API EuRIS;
17) scenariusze testów integracyjnych;
18) protokoły testów i odbioru integracji.

Generalny Wykonawca zobowiązany jest przeprowadzić testy integracji z EuRIS zgodnie z dokumentacją API, wymaganiami Zamawiającego oraz procedurami określonymi przez gestora albo administratora systemu EuRIS. Testy muszą obejmować co najmniej:

1) weryfikację możliwości uwierzytelnienia i autoryzacji;
2) weryfikację poprawności komunikacji z wymaganymi endpointami;
3) weryfikację poprawności mapowania danych;
4) weryfikację poprawności walidacji danych przed przekazaniem;
5) weryfikację poprawności przekazania danych testowych albo produkcyjnych, zgodnie z procedurami uzgodnionymi z Zamawiającym;
6) weryfikację obsługi odpowiedzi zwrotnych;
7) weryfikację obsługi błędów;
8) weryfikację działania mechanizmów monitorowania i alarmowania;
9) weryfikację logowania zdarzeń integracyjnych;
10) weryfikację zachowania integracji w przypadku niedostępności usługi zewnętrznej;
11) weryfikację ponowienia transmisji albo innej procedury obsługi danych nieprzekazanych;
12) weryfikację zgodności dokumentacji integracyjnej ze stanem faktycznym.

Jeżeli w toku realizacji zamówienia nastąpi zmiana dokumentacji API EuRIS, wymagań technicznych EuRIS, standardów RIS, procedur dostępu, procedur testowych albo wymagań gestora systemu EuRIS, Generalny Wykonawca zobowiązany jest przeanalizować wpływ tej zmiany na projektowane rozwiązanie, przedstawić Zamawiającemu ocenę skutków oraz zaproponować sposób dostosowania integracji, o ile zmiana mieści się w zakresie przedmiotu zamówienia albo jest niezbędna do osiągnięcia wymaganej zgodności systemu RIS.

Odbiór integracji z EuRIS może nastąpić wyłącznie po potwierdzeniu, że usługa integracyjna została uruchomiona, zabezpieczona, udokumentowana, przetestowana i przekazana do eksploatacji, a Zamawiający otrzymał kompletną dokumentację techniczną, testową, administracyjną i eksploatacyjną integracji.

1.2.16.4. Usługa przekazywania danych z wodowskazów systemu RIS do Systemu Hydrologii IMGW-PIB

1.2.16.4.1. Przedmiot i cel usługi

Generalny Wykonawca zrealizuje usługę przekazywania danych pomiarowych z wodowskazów systemu RIS do Systemu Hydrologii (SH) Instytutu Meteorologii i Gospodarki Wodnej – Państwowego Instytutu Badawczego, celem ich dalszego wykorzystania i publikacji w serwisie hydrologicznym IMGW-PIB dostępnym pod adresem hydro.imgw.pl.

Usługa musi obejmować automatyczne przekazywanie danych obserwacyjnych pochodzących z czujników hydrologicznych systemu RIS, w szczególności danych dotyczących:

1) stanu wody,
2) prześwitu mostu.

Zamawiający jest w posiadaniu dokumentacji technicznej interfejsu integracyjnego API Systemu Hydrologii (SH) Instytutu Meteorologii i Gospodarki Wodnej – Państwowego Instytutu Badawczego, którą przekaże Generalnemu Wykonawcy po podpisaniu Umowy. Generalny Wykonawca musi opracować, wdrożyć, uruchomić i przetestować usługę integracyjną zgodnie z przekazaną dokumentacją techniczną SH API, uzgodnieniami pomiędzy UŻŚ w Szczecinie oraz IMGW-PIB oraz wymaganiami określonymi w PFU.

1.2.16.4.2. Zakres lokalizacyjny i czujniki objęte integracją

Usługa musi objąć co najmniej następujące czujniki hydrologiczne systemu RIS:

Tabela 6: Wykaz lokalizacji czujników objętych integracją

Lp.	Lokalizacja czujnika
1.	Słubice – nabrzeże
2.	Kostrzyn nad Odrą – most drogowy nad Odrą
3.	Kostrzyn nad Odrą – most kolejowy 2 nad Wartą
4.	Siekierki – most kolejowy
5.	Osinów Dolny – most drogowy
6.	Krajnik Dolny – most drogowy
7.	Gryfino – most drogowy
8.	Mescherin – most drogowy
9.	Szczecin – Most Gryfitów
10.	Szczecin – Most Pionierów
11.	Szczecin – Most Portowy
12.	Szczecin – Most kolejowy Parnica
13.	Szczecin – most kolejowy Dworzec Główny

Generalny Wykonawca musi przyjąć, że powyższa lista stanowi zakres minimalny. Rozwiązanie musi umożliwiać zwiększenie liczby czujników objętych przekazywaniem danych bez konieczności modyfikacji kodu źródłowego usługi oraz bez udziału Generalnego Wykonawcy po zakończeniu wdrożenia.

1.2.16.4.3. Wymagania dotyczące metody przekazywania danych

Generalny Wykonawca musi zrealizować przekazywanie danych do Systemu Hydrologii IMGW-PIB z wykorzystaniem metody:

`WriteMany - /observation/write-many`

opisanej w dokumentacji technicznej SH API.

Usługa musi przekazywać dane w formacie JSON, zgodnie ze strukturą wymaganą przez SH API, obejmującą co najmniej:

1) identyfikator Obiektu SH,
2) kod parametru SH,
3) kolekcję danych pomiarowych,
4) datę i czas rekordu pomiarowego,
5) wartość rekordu pomiarowego,
6) informację o trybie nadpisywania danych, o ile wymaga tego konfiguracja integracji.

Generalny Wykonawca musi zapewnić mapowanie danych systemu RIS na strukturę wymaganą przez System Hydrologii, w tym mapowanie lokalnych identyfikatorów czujników RIS na identyfikatory Obiektów SH oraz mapowanie lokalnych typów pomiarów na kody parametrów SH właściwe dla stanu wody i prześwitu mostu.

Wartości przekazywane do SH API muszą być przekazywane w jednostkach, układzie odniesienia, dokładności oraz formacie uzgodnionym z IMGW-PIB. Generalny Wykonawca musi uwzględnić w projekcie usługi konieczność rozróżnienia danych dotyczących stanu wody oraz danych dotyczących prześwitu mostu jako odrębnych parametrów pomiarowych.

1.2.16.4.4. Wymagania dotyczące konfiguracji czujników i metadanych

Usługa musi posiadać mechanizm administracyjny umożliwiający Zamawiającemu samodzielne wskazywanie czujników, z których dane mają być przekazywane do Systemu Hydrologii. Mechanizm ten musi działać bez konieczności udziału Generalnego Wykonawcy, bez modyfikacji kodu źródłowego oraz bez ponownego wdrażania aplikacji.

Dla każdego czujnika Zamawiający musi mieć możliwość wprowadzenia, edycji, dezaktywacji i usunięcia konfiguracji obejmującej co najmniej:

1) lokalny identyfikator czujnika w systemie RIS,
2) status przekazywania danych do SH: aktywny / nieaktywny,
3) zakres przekazywanych parametrów: stan wody, prześwit mostu,
4) identyfikator Obiektu SH,
5) kod parametru SH dla stanu wody,
6) kod parametru SH dla prześwitu mostu,
7) tryb obsługi nadpisywania danych,
8) częstotliwość przekazywania danych,
9) reguły walidacji danych,
10) datę rozpoczęcia i zakończenia obowiązywania konfiguracji.

Dla każdego czujnika Zamawiający musi mieć możliwość wprowadzenia metadanych identyfikujących czujnik w Systemie Hydrologii, obejmujących co najmniej:

1) pełną nazwę stacji,
2) skróconą nazwę stacji,
3) współrzędne geograficzne,
4) nazwę rzeki,
5) województwo,
6) kilometr biegu według MPHP,
7) rzędną zera,
8) powiat,
9) gminę,
10) powierzchnię zlewni po wodowskaz.

Usługa musi zapewniać walidację kompletności i poprawności metadanych przed aktywacją przekazywania danych dla danego czujnika. W przypadku braku wymaganych metadanych system musi uniemożliwić aktywację przekazywania danych dla danego czujnika oraz wskazać administratorowi zakres braków.

1.2.16.4.5. Wymagania dotyczące harmonogramu i trybu pracy usługi

Usługa musi działać w sposób automatyczny, cykliczny i bezobsługowy. Generalny Wykonawca musi umożliwić konfigurowanie częstotliwości przekazywania danych dla poszczególnych czujników lub grup czujników.

Usługa musi obsługiwać co najmniej następujące tryby przekazywania danych:

1) przekazywanie bieżących danych pomiarowych,
2) ponowienie przekazania danych w przypadku błędu komunikacji,
3) uzupełnienie danych zaległych po okresowej niedostępności systemu RIS, sieci transmisyjnej lub SH API,
4) ręczne wymuszenie ponownej wysyłki danych dla wskazanego czujnika, parametru i przedziału czasu przez uprawnionego administratora.

Generalny Wykonawca musi zapewnić mechanizm kolejkowania danych, który zabezpieczy przed utratą danych w przypadku czasowej niedostępności SH API lub łączności pomiędzy systemem RIS a Systemem Hydrologii.

1.2.16.4.6. Wymagania dotyczące bezpieczeństwa i autoryzacji

Generalny Wykonawca musi zrealizować komunikację z SH API z wykorzystaniem mechanizmów autoryzacji i autentykacji określonych w dokumentacji technicznej SH API oraz przekazanych przez Zamawiającego danych dostępowych.

Dane uwierzytelniające do SH API muszą być przechowywane w sposób bezpieczny, z wyłączeniem możliwości ich odczytu przez nieuprawnionych użytkowników systemu. Hasła, tokeny, sekrety i inne dane dostępowe nie mogą być zapisywane w kodzie źródłowym, plikach konfiguracyjnych w postaci jawnej ani w logach aplikacyjnych.

Usługa musi zapewniać rozliczalność działań administracyjnych, w tym rejestrowanie informacji o użytkowniku, czasie i zakresie każdej zmiany konfiguracji czujnika, metadanych, parametrów przekazywania danych oraz danych dostępowych do interfejsu SH API.

1.2.16.4.7. Wymagania dotyczące walidacji i jakości danych

Generalny Wykonawca musi zapewnić walidację danych przed ich przekazaniem do SH API. Walidacja musi obejmować co najmniej:

1) sprawdzenie kompletności danych pomiarowych,

2) sprawdzenie zgodności daty i czasu z formatem wymaganym przez SH API,
3) sprawdzenie przekazywania czasu w UTC,
4) sprawdzenie poprawności formatu wartości liczbowych,
5) sprawdzenie przypisania pomiaru do aktywnego czujnika,
6) sprawdzenie przypisania pomiaru do właściwego parametru SH,
7) sprawdzenie zakresu dopuszczalnych wartości pomiarowych,
8) wykrywanie wartości pustych, błędnych, skrajnych lub nieaktualnych.

Dane niespełniające reguł walidacji nie mogą zostać przekazane do SH API. System musi zarejestrować takie zdarzenie w logach technicznych i udostępnić informację administratorowi w panelu administracyjnym lub module monitorowania integracji.

1.2.16.4.8. Wymagania dotyczące monitorowania, logowania i obsługi błędów

Usługa musi posiadać mechanizmy monitorowania poprawności działania integracji. Generalny Wykonawca musi zapewnić rejestrowanie co najmniej następujących informacji:

1) data i czas uruchomienia cyklu przekazywania danych,
2) lista czujników objętych danym cyklem,
3) liczba rekordów przygotowanych do wysłania,
4) liczba rekordów poprawnie przekazanych,
5) liczba rekordów odrzuconych na etapie walidacji,
6) liczba rekordów nieprzekazanych z powodu błędu komunikacji,
7) odpowiedzi SH API,
8) kody błędów zwracane przez SH API,
9) liczba ponowień wysyłki,
10) data i czas ostatniej poprawnej wysyłki dla każdego czujnika i parametru.

System musi obsługiwać błędy zwracane przez SH API, w tym błędy autoryzacji, błędy uprawnień, błędy niepoprawnego adresu usługi, błędy warunków początkowych oraz błędy po stronie serwera API. Dla każdego typu błędu usługa musi zapewnić odpowiednią reakcję, obejmującą rejestrację zdarzenia, oznaczenie statusu wysyłki, ponowienie wysyłki w przypadkach technicznie uzasadnionych oraz powiadomienie administratora.

1.2.16.4.9. Wymagania dotyczące panelu administracyjnego

Generalny Wykonawca musi zapewnić Zamawiającemu narzędzie administracyjne do zarządzania usługą przekazywania danych do SH API. Narzędzie musi umożliwiać co najmniej:

1) dodawanie nowych czujników do integracji,
2) edycję konfiguracji istniejących czujników,
3) aktywację i dezaktywację przekazywania danych dla czujnika,
4) konfigurację metadanych czujnika,
5) konfigurację identyfikatorów Obiektów SH i kodów parametrów SH,
6) konfigurację harmonogramu przekazywania danych,
7) podgląd statusu ostatniej wysyłki,
8) podgląd historii wysyłek,
9) podgląd błędów i ostrzeżeń,
10) ręczne ponowienie wysyłki danych,
11) eksport konfiguracji i historii działania integracji do pliku.

Dostęp do narzędzia administracyjnego musi być ograniczony do uprawnionych użytkowników. System musi umożliwiać nadawanie uprawnień co najmniej w podziale na użytkowników posiadających prawo podglądu konfiguracji oraz użytkowników posiadających prawo zmiany konfiguracji.

1.2.16.4.10. Wymagania dotyczące dokumentacji

Generalny Wykonawca opracuje i przekaże Zamawiającemu dokumentację techniczną, administracyjną i eksploatacyjną usługi przekazywania danych do Systemu Hydrologii IMGW-PIB.

Dokumentacja musi obejmować co najmniej:

1) opis architektury usługi,
2) opis przepływu danych pomiędzy systemem RIS a SH API,
3) opis mapowania danych RIS na strukturę SH API,
4) opis konfiguracji czujników i metadanych,
5) opis mechanizmu autoryzacji i przechowywania danych dostępowych,
6) opis harmonogramu przekazywania danych,
7) opis mechanizmów kolejkowania i ponawiania wysyłki,
8) opis walidacji danych,
9) opis obsługi błędów,
10) instrukcję administratora,
11) instrukcję odtworzenia usługi po awarii,
12) scenariusze testów integracyjnych i odbiorowych,

13) wykaz parametrów konfiguracyjnych,
14) wykaz logów, komunikatów i kodów błędów.

1.2.16.4.11. Wymagania dotyczące testów i odbioru

Generalny Wykonawca przeprowadzi testy integracyjne, funkcjonalne, bezpieczeństwa i eksploatacyjne usługi przekazywania danych do SH API. Testy muszą zostać przeprowadzone z udziałem Zamawiającego, a w zakresie wymagającym potwierdzenia poprawności przyjęcia danych przez System Hydrologii także z uwzględnieniem uzgodnień z IMGW-PIB.

Testy odbiorowe muszą obejmować co najmniej:

1) przekazanie danych stanu wody dla każdego czujnika objętego zakresem minimalnym,
2) przekazanie danych prześwitu mostu dla każdego czujnika objętego zakresem minimalnym, dla którego taki pomiar występuje,
3) poprawność mapowania lokalnych identyfikatorów RIS na identyfikatory Obiektów SH,
4) poprawność mapowania typów pomiarów na kody parametrów SH,
5) poprawność formatu JSON,
6) poprawność formatu daty i czasu,
7) przekazywanie czasu w UTC,
8) obsługę trybu nadpisywania danych,
9) reakcję systemu na brak łączności z SH API,
10) ponowienie wysyłki po przywróceniu dostępności SH API,
11) obsługę błędnych danych pomiarowych,
12) obsługę błędnych danych konfiguracyjnych,
13) dodanie nowego czujnika przez administratora bez udziału Generalnego Wykonawcy,
14) dezaktywację czujnika przez administratora,
15) zmianę metadanych czujnika przez administratora,
16) rejestrację historii wysyłek i błędów,
17) kontrolę dostępu do funkcji administracyjnych.

Warunkiem odbioru usługi jest potwierdzenie, że dane z czujników RIS objętych zakresem wdrożenia są poprawnie przygotowywane, walidowane, przekazywane do SH API oraz możliwe do wykorzystania po stronie Systemu Hydrologii IMGW-PIB zgodnie z uzgodnionym zakresem integracji.

1.2.16.4.12. Wymagania dotyczące skalowalności i utrzymania

Usługa musi być skalowalna w zakresie liczby obsługiwanych czujników, liczby parametrów pomiarowych, częstotliwości przekazywania danych oraz liczby rekordów przetwarzanych w jednym cyklu wysyłki.

Generalny Wykonawca musi zapewnić możliwość rozbudowy konfiguracji o kolejne czujniki hydrologiczne systemu RIS oraz kolejne parametry pomiarowe bez konieczności zmiany architektury rozwiązania. Rozwiązanie musi umożliwiać utrzymanie i dalszą eksploatację przez Zamawiającego po zakończeniu realizacji Umowy, w tym samodzielną zmianę konfiguracji, analizę błędów, odtwarzanie wysyłek oraz weryfikację historii przekazanych danych.

1.2.16.5. API systemu RIS i udostępnianie danych dziedzinowych

Generalny Wykonawca zobowiązany jest zaprojektować, wykonać, uruchomić, udokumentować, zabezpieczyć, przetestować i przekazać do eksploatacji API systemu RIS umożliwiające pobieranie danych dziedzinowych z systemu RIS przez systemy własne Zamawiającego oraz systemy teleinformatyczne innych instytucji uprawnionych do korzystania z tych danych.

API systemu RIS musi stanowić udokumentowany, stabilny i możliwy do utrzymania interfejs integracyjny, umożliwiający kontrolowane udostępnianie danych dziedzinowych bez konieczności bezpośredniego dostępu do baz danych, komponentów wewnętrznych, urządzeń terenowych albo nieudokumentowanych mechanizmów systemu RIS.

API musi umożliwiać udostępnianie danych co najmniej w następujących trybach, jeżeli zostaną przewidziane w dokumentacji projektowej:

1) pobieranie danych na żądanie przez uprawniony system zewnętrzny;
2) pobieranie danych według zakresu czasowego;
3) pobieranie danych według lokalizacji, urządzenia, punktu pomiarowego, typu danych albo kategorii danych;
4) pobieranie danych aktualnych;
5) pobieranie danych historycznych;
6) pobieranie metadanych, słowników i identyfikatorów;
7) przekazywanie informacji o statusie dostępności danych albo statusie źródła danych.

Zakres danych udostępnianych przez API musi zostać określony na etapie analizy przedwdrożeniowej i projektowania, z uwzględnieniem wymagań Zamawiającego, przepisów prawa, wymagań bezpieczeństwa, wymagań ochrony danych, wymagań interesariuszy oraz architektury systemu RIS. Zakres ten powinien obejmować co najmniej dane dziedzinowe gromadzone i przetwarzane w systemie RIS, które Zamawiający zamierza publikować, udostępniać albo wykorzystywać w systemach własnych i systemach instytucji współpracujących.

API musi zapewniać co najmniej:

1) uwierzytelnianie systemów i użytkowników technicznych korzystających z API;
2) autoryzację dostępu do określonych kategorii danych;
3) możliwość definiowania zakresu danych dostępnego dla danego odbiorcy;
4) szyfrowanie transmisji;
5) rejestrowanie wywołań API;
6) rejestrowanie błędów, odrzuceń i nieudanych prób dostępu;
7) limity techniczne chroniące system RIS przed nadmiernym obciążeniem;
8) mechanizmy wersjonowania interfejsu;
9) mechanizmy monitorowania dostępności API;
10) dokumentację techniczną i przykłady użycia.

API musi być zaprojektowane w sposób umożliwiający rozróżnienie danych według źródła, czasu pomiaru, czasu przetworzenia, czasu publikacji, statusu jakości i statusu korekty. Dane udostępniane przez API muszą zawierać metadane niezbędne do ich prawidłowej interpretacji przez systemy zewnętrzne.

Generalny Wykonawca zobowiązany jest zapewnić dokumentację API obejmującą co najmniej:

1) opis przeznaczenia API;
2) opis zakresu udostępnianych danych;
3) opis modelu danych;
4) opis struktur komunikatów;
5) opis parametrów zapytań;
6) opis odpowiedzi;
7) opis kodów błędów;
8) opis mechanizmów uwierzytelniania i autoryzacji;
9) opis limitów technicznych;
10) opis wersjonowania;
11) opis reguł walidacji;
12) opis słowników i identyfikatorów;
13) przykładowe zapytania i odpowiedzi;
14) procedury nadawania, zmiany i cofania dostępu;
15) procedury utrzymania, monitorowania i obsługi błędów.

API systemu RIS musi być przygotowane do wykorzystania przez różne kategorie odbiorców danych, w szczególności przez systemy Zamawiającego, systemy innych jednostek administracji publicznej, systemy instytucji odpowiedzialnych za bezpieczeństwo żeglugi, systemy hydrologiczne, systemy mapowe, portale informacyjne, usługi cyfrowe oraz inne systemy uprawnione do korzystania z danych RIS.

Udostępnianie danych przez API musi odbywać się zgodnie z zasadą minimalnego niezbędnego zakresu dostępu. Każdy odbiorca danych powinien otrzymywać dostęp wyłącznie do takich kategorii danych, zakresów terytorialnych, zakresów czasowych i funkcji API, które wynikają z jego uprawnień, uzgodnień, przepisów prawa albo decyzji Zamawiającego.

Generalny Wykonawca zobowiązany jest zapewnić możliwość testowania API przez Zamawiającego i wskazane przez Zamawiającego podmioty, w tym przez przygotowanie środowiska testowego albo uzgodnionego trybu testów integracyjnych. Testy API muszą obejmować poprawność danych, kompletność danych, jakość danych, obsługę błędów, bezpieczeństwo, wydajność, limity, wersjonowanie, dokumentację oraz zgodność ze stanem faktycznym systemu RIS.

1.2.16.6. Dokumentacja, bezpieczeństwo, testy i odbiór integracji

Generalny Wykonawca zobowiązany jest opracować dokumentację interoperacyjności, danych i integracji systemu RIS. Dokumentacja ta musi obejmować co najmniej:

1) architekturę integracyjną systemu RIS;
2) model danych systemu RIS;
3) opis źródeł danych;
4) opis odbiorców danych;
5) wykaz interfejsów wewnętrznych i zewnętrznych;
6) dokumentację API systemu RIS;
7) dokumentację integracji z EuRIS;
8) dokumentację integracji z Systemem Hydrologii IMGW-PIB;
9) opis słowników, kodów, identyfikatorów i danych referencyjnych;
10) opis reguł walidacji danych;
11) opis zasad jakości danych;
12) opis zasad bezpieczeństwa wymiany danych;
13) opis zasad monitorowania integracji;
14) opis zasad obsługi błędów integracyjnych;
15) opis zasad wersjonowania interfejsów i danych;
16) procedury eksploatacyjne;
17) procedury nadawania, zmiany i odbierania dostępu do API;
18) scenariusze testów integracyjnych i interoperacyjności.

Wymiana danych z systemami zewnętrznymi musi być objęta mechanizmami bezpieczeństwa adekwatnymi do charakteru danych, sposobu integracji, kategorii odbiorcy oraz ryzyka związanego z nieuprawnionym dostępem, utratą integralności danych, niedostępnością interfejsu albo błędną publikacją danych. Wymagania bezpieczeństwa muszą obejmować co najmniej uwierzytelnianie, autoryzację, szyfrowanie transmisji, logowanie zdarzeń, monitorowanie, alarmowanie, kontrolę uprawnień, rozliczalność działań i ochronę przed nadużyciami.

W ramach odbioru Generalny Wykonawca zobowiązany jest przeprowadzić testy interoperacyjności, danych i integracji. Testy muszą obejmować co najmniej:

1) weryfikację modelu danych;
2) weryfikację słowników, kodów i identyfikatorów;
3) weryfikację poprawności danych źródłowych i danych udostępnianych;
4) weryfikację walidacji danych;
5) weryfikację jakości i kompletności danych;
6) weryfikację integracji z EuRIS;
7) weryfikację integracji z Systemem Hydrologii IMGW-PIB;
8) weryfikację działania API systemu RIS;
9) weryfikację bezpieczeństwa interfejsów;
10) weryfikację monitorowania integracji;
11) weryfikację alarmowania o błędach integracji;
12) weryfikację obsługi błędów i ponawiania transmisji, jeżeli ma zastosowanie;
13) weryfikację dokumentacji technicznej i eksploatacyjnej;
14) weryfikację zgodności dokumentacji ze stanem faktycznym.

Odbiór integracji i API może nastąpić wyłącznie po potwierdzeniu, że wszystkie wymagane interfejsy zostały uruchomione, zabezpieczone, udokumentowane, przetestowane i przekazane do eksploatacji, a Zamawiający otrzymał kompletną dokumentację techniczną, eksploatacyjną, testową i administracyjną.

Rezultatem realizacji wymagań określonych w niniejszym rozdziale musi być zmodernizowany system RIS zdolny do spójnego, bezpiecznego, kontrolowanego i udokumentowanego udostępniania danych dziedzinowych Zamawiającemu, systemom europejskim, systemom administracji publicznej oraz innym uprawnionym interesariuszom, przy zachowaniu wymagań interoperacyjności, jakości danych, bezpieczeństwa, rozliczalności i możliwości dalszej rozbudowy.

1.2.17. Dostępność cyfrowa

Generalny Wykonawca zobowiązany jest zapewnić dostępność cyfrową dostarczanych, modernizowanych, konfigurowanych, integrowanych i wdrażanych rozwiązań aplikacyjnych oraz

usług cyfrowych systemu RIS, w zakresie w jakim rozwiązania te są udostępniane użytkownikom końcowym, użytkownikom zewnętrznym, użytkownikom administracji publicznej, użytkownikom Centrum RIS, administratorom, operatorom, interesariuszom zewnętrznym albo innym osobom korzystającym z interfejsów systemu.

Wymagania dostępności cyfrowej dotyczą w szczególności:

1) usług cyfrowych udostępnianych użytkownikom śródlądowych dróg wodnych;
2) aplikacji VTT;
3) aplikacji hydrometeorologicznej;
4) aplikacji do zarządzania usługami i sensorami systemu RIS;
5) paneli administracyjnych;
6) interfejsów operatorskich;
7) interfejsów użytkowników zewnętrznych;
8) formularzy elektronicznych;
9) komunikatów, powiadomień i treści publikowanych przez system;
10) dokumentów elektronicznych generowanych albo udostępnianych przez system;
11) komponentów wizualizacji danych, wykresów, tabel, map, warstw przestrzennych i widoków analitycznych;
12) instrukcji użytkownika, materiałów szkoleniowych, pomocy kontekstowej i dokumentacji przeznaczonej dla użytkowników systemu.

Generalny Wykonawca zobowiązany jest zapewnić zgodność rozwiązań z ustawą z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych, z wymaganiami wynikającymi z Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/2102, z normą EN 301 549 w aktualnej wersji mającej zastosowanie do danego zakresu zamówienia oraz z wymaganiami WCAG na poziomie nie niższym niż 2.1 AA. Dla nowych i modernizowanych rozwiązań aplikacyjnych Zamawiający wymaga uwzględnienia również kryteriów WCAG 2.2 na poziomie AA, o ile są możliwe do zastosowania i nie pozostają w sprzeczności z aktualnie obowiązującymi wymaganiami prawnymi lub normą zharmonizowaną.

Jeżeli dostarczane przez Generalnego Wykonawcę produkty, usługi, komponenty aplikacyjne, terminale, interfejsy, aplikacje lub usługi cyfrowe mieszczą się w zakresie ustawy z dnia 26 kwietnia 2024 r. o zapewnianiu spełniania wymagań dostępności niektórych produktów i usług przez podmioty gospodarcze, Generalny Wykonawca zobowiązany jest zapewnić ich zgodność również z wymaganiami tej ustawy oraz z Dyrektywą Parlamentu Europejskiego i Rady (UE) 2019/882 w zakresie mającym zastosowanie do przedmiotu zamówienia.

Dostępność cyfrowa musi być zapewniona od etapu analizy, projektowania UX/UI i architektury informacji, przez implementację, testy, odbiór, wdrożenie, szkolenia, dokumentację, utrzymanie, rozwój i aktualizacje systemu. Niedopuszczalne jest traktowanie dostępności cyfrowej wyłącznie

jako końcowej korekty graficznej albo jednorazowego testu wykonanego po zakończeniu implementacji.

Interfejsy użytkownika muszą być projektowane zgodnie z zasadami: postrzegalności, funkcjonalności, zrozumiałości i solidności / kompatybilności. Oznacza to w szczególności, że treści i funkcje systemu muszą być możliwe do odbioru, obsługi, zrozumienia i wykorzystania przez osoby z różnymi potrzebami funkcjonalnymi, w tym osoby korzystające z czytników ekranu, klawiatury, powiększenia ekranu, wysokiego kontrastu, alternatywnych metod wprowadzania danych oraz innych technologii wspomagających.

Generalny Wykonawca zobowiązany jest zapewnić co najmniej następujące wymagania funkcjonalne dostępności cyfrowej:

1) pełną obsługę podstawowych funkcji systemu z użyciem klawiatury, bez konieczności korzystania z myszy;
2) logiczną i przewidywalną kolejność fokusu;
3) widoczny fokus klawiaturowy dla elementów interaktywnych;
4) możliwość pominięcia powtarzalnych bloków nawigacyjnych;
5) poprawne semantycznie nagłówki, listy, tabele, formularze i elementy interfejsu;
6) etykiety i instrukcje dla pól formularzy;
7) jednoznaczną identyfikację błędów formularzy oraz zrozumiałe komunikaty walidacyjne;
8) możliwość poprawy błędów przed wysłaniem formularza albo zatwierdzeniem operacji;
9) odpowiedni kontrast tekstu, elementów interaktywnych, ikon i informacji graficznych;
10) możliwość powiększania treści bez utraty funkcjonalności i czytelności;
11) responsywność interfejsu i dostosowanie do różnych rozdzielczości oraz urządzeń;
12) brak przekazywania informacji wyłącznie kolorem, położeniem, kształtem albo dźwiękiem;
13) alternatywy tekstowe dla treści nietekstowych, ikon, przycisków, grafik, wykresów i informacji wizualnych;
14) podpisy, transkrypcje albo inne alternatywy dla materiałów multimedialnych, jeżeli takie materiały są dostarczane w ramach systemu;
15) brak elementów migających lub błyskających w sposób mogący powodować zagrożenie dla użytkowników;
16) zrozumiałe tytuły stron, nazwy widoków, opisy sekcji i nazwy linków;
17) spójną nawigację i spójne nazewnictwo elementów interfejsu;
18) poprawną współpracę z technologiami wspomagającymi;
19) komunikaty statusowe możliwe do odczytania przez technologie wspomagające;
20) możliwość korzystania z systemu bez ograniczeń czasowych albo z możliwością ich wydłużenia, jeżeli ograniczenia czasowe są konieczne ze względów bezpieczeństwa.

W przypadku aplikacji mapowych, wizualizacji sytuacji na drodze wodnej, wykresów, tabel, dashboardów, danych hydrologicznych, meteorologicznych, AIS/VTT i informacji przestrzennych Generalny Wykonawca zobowiązany jest zapewnić alternatywne sposoby dostępu do informacji. W szczególności dane prezentowane graficznie muszą być możliwe do odczytu również w formie tekstowej, tabelarycznej, opisowej albo przez interfejs API, jeżeli jest to uzasadnione charakterem danych i wymaganiami użytkowników.

Jeżeli pełna dostępność wybranych specjalistycznych komponentów mapowych, operatorskich, technicznych albo wizualizacyjnych nie jest możliwa z przyczyn obiektywnych, Generalny Wykonawca zobowiązany jest:

1) wykazać przyczynę ograniczenia;
2) wskazać zakres niedostępności;
3) zaproponować rozwiązanie alternatywne;
4) uzyskać akceptację Zamawiającego;
5) opisać ograniczenie i sposób alternatywnego dostępu w dokumentacji;
6) zapewnić, aby ograniczenie nie dotyczyło podstawowych usług cyfrowych udostępnianych publicznie, chyba że przepisy dopuszczają wyjątek.

Dokumenty elektroniczne generowane albo udostępniane przez system, w szczególności raporty, zestawienia, komunikaty, instrukcje, dokumentacja użytkownika, pliki PDF, arkusze i dokumenty tekstowe, muszą być przygotowywane w sposób dostępny cyfrowo. Wymaganie obejmuje co najmniej poprawną strukturę dokumentu, nagłówki, tekst alternatywny dla istotnych grafik, właściwą kolejność odczytu, tabele z nagłówkami, język dokumentu, tagowanie dokumentów PDF, dostępne formularze, metadane oraz brak skanów tekstu bez warstwy tekstowej.

Treści publikowane w usługach cyfrowych systemu RIS muszą być redagowane w sposób zrozumiały, logicznie uporządkowany i możliwy do odczytania przez technologie wspomagające. Dotyczy to w szczególności komunikatów dla użytkowników, informacji hydrologicznych i meteorologicznych, instrukcji, ostrzeżeń, komunikatów błędów, komunikatów statusowych, informacji o awariach i dostępności usług.

Generalny Wykonawca zobowiązany jest zapewnić dostępność cyfrową dokumentacji użytkownika, pomocy kontekstowej, materiałów szkoleniowych oraz instrukcji obsługi systemu. Materiały te muszą być przekazane w formatach umożliwiających korzystanie przez osoby ze szczególnymi potrzebami, w tym przez osoby korzystające z technologii wspomagających.

Generalny Wykonawca zobowiązany jest przeprowadzić testy dostępności cyfrowej przed odbiorem każdego rozwiązania aplikacyjnego i każdej usługi cyfrowej. Testy muszą obejmować co najmniej:

1) testy automatyczne z wykorzystaniem narzędzi do oceny dostępności;
2) testy manualne kluczowych ścieżek użytkownika;
3) testy obsługi klawiaturą;

4) testy współpracy z czytnikami ekranu;
5) testy kontrastu;
6) testy responsywności;
7) testy formularzy i komunikatów błędów;
8) testy dokumentów elektronicznych generowanych przez system;
9) testy dostępności komponentów mapowych, tabelarycznych, wykresów i dashboardów;
10) testy dostępności w zakresie reprezentatywnych ról użytkowników.

Testy automatyczne nie mogą stanowić jedynej podstawy potwierdzenia dostępności cyfrowej. Wyniki testów automatycznych muszą być uzupełnione testami manualnymi i oceną ekspercką, obejmującą co najmniej kluczowe procesy i ścieżki użytkownika wskazane przez Zamawiającego.

Generalny Wykonawca zobowiązany jest opracować i przekazać Zamawiającemu raport z audytu dostępności cyfrowej dla każdej aplikacji, usługi cyfrowej albo istotnego komponentu interfejsu użytkownika. Raport musi obejmować co najmniej:

1) zakres audytu;
2) datę wykonania audytu;
3) wersję badanego rozwiązania;
4) zastosowane standardy i kryteria oceny;
5) wykorzystane narzędzia;
6) wykaz badanych widoków, procesów i dokumentów;
7) wykaz stwierdzonych niezgodności;
8) klasyfikację istotności niezgodności;
9) rekomendacje naprawcze;
10) informację o usunięciu niezgodności;
11) wynik ponownej weryfikacji;
12) oświadczenie o zgodności albo wykaz pozostałych ograniczeń wraz z uzasadnieniem i sposobem alternatywnego dostępu.

Generalny Wykonawca zobowiązany jest przygotować informacje niezbędne do sporządzenia lub aktualizacji deklaracji dostępności dla publicznie udostępnianych stron internetowych, aplikacji mobilnych, portali i usług cyfrowych objętych obowiązkiem wynikającym z przepisów. Zakres tych informacji musi być zgodny z obowiązującym wzorem i wymaganiami dla deklaracji dostępności.

W okresie gwarancji oraz w okresie świadczenia usług utrzymania Generalny Wykonawca zobowiązany jest utrzymywać dostępność cyfrową dostarczonych rozwiązań. Każda zmiana interfejsu, funkcji, szablonu, komponentu frontendowego, formularza, widoku mapowego, raportu, dokumentu generowanego przez system albo treści publikowanej w systemie musi być oceniona pod kątem wpływu na dostępność cyfrową.

Stwierdzone niezgodności dostępności cyfrowej muszą być usuwane przez Generalnego Wykonawcę w ramach procedury obsługi błędów i zmian, z priorytetem adekwatnym do wpływu niezgodności na możliwość korzystania z usługi przez użytkowników. Niezgodności uniemożliwiające wykonanie podstawowej czynności przez osoby korzystające z technologii wspomagających należy traktować jako istotne wady funkcjonalne.

Generalny Wykonawca zobowiązany jest zapewnić, aby komponenty zewnętrzne, biblioteki interfejsu, szablony, frameworki, kontrolki formularzy, komponenty mapowe, komponenty wykresów, odtwarzacze multimedialne, mechanizmy autoryzacji i inne elementy wpływające na interfejs użytkownika były dobrane, skonfigurowane i wykorzystane w sposób umożliwiający spełnienie wymagań dostępności cyfrowej.

Odbiór aplikacji albo usługi cyfrowej może nastąpić wyłącznie po przekazaniu raportu z audytu dostępności cyfrowej, usunięciu niezgodności krytycznych i wysokich oraz potwierdzeniu, że rozwiązanie spełnia wymagania dostępności cyfrowej określone w PFU, przepisach prawa, normie EN 301 549 oraz WCAG na wymaganym poziomie.

1.2.18. Cyberbezpieczeństwo, kontrola dostępu, monitoring i logowanie

Generalny Wykonawca zobowiązany jest zaprojektować, wykonać, dostarczyć, skonfigurować, uruchomić, przetestować i przekazać do eksploatacji wszystkie komponenty systemu RIS w sposób zapewniający wymagany poziom cyberbezpieczeństwa, kontroli dostępu, monitoringu bezpieczeństwa, monitoringu technicznego, logowania zdarzeń, rozliczalności działań oraz odporności na awarie, nadużycia i nieuprawniony dostęp.

Wymagania określone w niniejszym rozdziale mają charakter przekrojowy i dotyczą wszystkich elementów przedmiotu zamówienia, w szczególności:

1) usług cyfrowych systemu RIS;
2) API systemu RIS i interfejsów integracyjnych;
3) integracji z systemami zewnętrznymi, w tym z EuRIS oraz Systemem Hydrologii IMGW-PIB;
4) systemu monitoringu wizyjnego CCTV;
5) systemu łączności radiowej VHF/AIS/DGNSS;
6) czujników hydrologicznych i sensorów meteorologicznych;
7) lokalnych komponentów akwizycji, buforowania i przekazywania danych;
8) sieci transmisji danych;
9) urządzeń sieciowych, routerów, modemów, zapór, przełączników, urządzeń VPN i urządzeń transmisyjnych;

10) szaf teletechnicznych typu zewnętrznego oraz ich wyposażenia;
11) systemów zasilania, UPS, listew zasilających, liczników energii oraz systemów monitoringu środowiskowego;
12) serwerowni głównej, serwerowni zapasowej i łącza pomiędzy tymi lokalizacjami;
13) infrastruktury serwerowej, wirtualizacyjnej, macierzowej, backupowej i replikacyjnej;
14) systemów monitoringu technicznego zasobów infrastrukturalnych i aplikacyjnych;
15) stacji operatorskich, stacji klienckich, paneli administracyjnych i konsol zarządzających;
16) dokumentacji, konfiguracji, skryptów, kont technicznych, kont serwisowych, certyfikatów, kluczy, tokenów, licencji i repozytoriów konfiguracji.

Wymagania cyberbezpieczeństwa muszą być stosowane na wszystkich etapach realizacji zamówienia, tj. podczas analizy, projektowania, dostaw, instalacji, konfiguracji, integracji, migracji, testów, odbiorów, dokumentowania, szkolenia, wdrożenia produkcyjnego, świadczenia gwarancji, obsługi serwisowej i utrzymania. Niedopuszczalne jest traktowanie cyberbezpieczeństwa wyłącznie jako czynności końcowej wykonywanej po zakończeniu konfiguracji albo wdrożenia.

Generalny Wykonawca zobowiązany jest stosować zasadę bezpieczeństwa w fazie projektowania i domyślnej bezpiecznej konfiguracji. Wszystkie komponenty systemu RIS muszą być dostarczone i skonfigurowane w sposób ograniczający powierzchnię ataku, minimalizujący liczbę aktywnych usług, portów, kont i interfejsów oraz zapewniający kontrolowany, udokumentowany i rozliczalny dostęp administracyjny, operatorski, serwisowy i integracyjny.

Rozwiązania wdrażane przez Generalnego Wykonawcę muszą być zgodne z wymaganiami prawnymi, normatywnymi i technicznymi wskazanymi w PFU, w szczególności w zakresie cyberbezpieczeństwa, ochrony danych, komunikacji elektronicznej, interoperacyjności, bezpieczeństwa aplikacji, bezpieczeństwa API, bezpieczeństwa urządzeń połączonych, bezpieczeństwa automatyki i urządzeń terenowych oraz ciągłości działania.

1.2.18.1. Zakres odpowiedzialności Generalnego Wykonawcy

Generalny Wykonawca ponosi odpowiedzialność za cyberbezpieczeństwo wszystkich komponentów, które dostarcza, instaluje, konfiguruje, modernizuje, rekonfiguruje, integruje albo obejmuje odpowiedzialnością gwarancyjną lub serwisową.

W przypadku wykorzystania istniejących zasobów systemu RIS Generalny Wykonawca zobowiązany jest określić w dokumentacji projektowej i powykonawczej:

1) które zasoby istniejące są wykorzystywane bez ingerencji;
2) które zasoby istniejące są rekonfigurowane;
3) które zasoby istniejące są integrowane z nowymi komponentami;
4) które zasoby istniejące są objęte odpowiedzialnością Generalnego Wykonawcy;
5) które zasoby pozostają poza zakresem odpowiedzialności Generalnego Wykonawcy;

6) jakie ryzyka bezpieczeństwa wynikają z powiązania nowych komponentów z zasobami istniejącymi;
7) jakie środki zabezpieczające należy zastosować w celu ograniczenia tych ryzyk.

Generalny Wykonawca zobowiązany jest wykonać analizę bezpieczeństwa projektowanej architektury systemu RIS w zakresie objętym zamówieniem. Analiza musi obejmować co najmniej identyfikację zasobów, stref bezpieczeństwa, kanałów komunikacyjnych, punktów styku z systemami zewnętrznymi, kont uprzywilejowanych, interfejsów administracyjnych, interfejsów API, komponentów terenowych, komponentów centralnych, usług krytycznych, mechanizmów monitorowania, logowania i odtwarzania po awarii.

1.2.18.2. Segmentacja, strefy bezpieczeństwa i separacja ruchu

Architektura systemu RIS musi zostać zaprojektowana z zastosowaniem segmentacji logicznej i funkcjonalnej. Generalny Wykonawca zobowiązany jest wyodrębnić strefy i kanały komunikacyjne odpowiednie dla funkcji, poziomu ryzyka, rodzaju danych, lokalizacji komponentów oraz sposobu eksploatacji systemu.

Segmentacja musi obejmować co najmniej:

1) strefę systemów centralnych Centrum RIS;
2) strefę serwerowni zapasowej;
3) strefę usług cyfrowych i API;
4) strefę integracji z systemami zewnętrznymi;
5) strefę systemu monitoringu wizyjnego CCTV;
6) strefę systemu VHF/AIS/DGNSS;
7) strefę czujników hydrologicznych i sensorów meteorologicznych;
8) strefę lokalnych komponentów akwizycji danych;
9) strefę zarządzania urządzeniami terenowymi;
10) strefę monitoringu technicznego;
11) strefę administracyjną;
12) strefę dostępu operatorskiego;
13) strefę transmisji danych pomiędzy lokalizacjami terenowymi a Centrum RIS;
14) strefę transmisji pomiędzy serwerownią główną i zapasową;
15) strefę dostępu serwisowego i zdalnego utrzymania.

Ruch sieciowy pomiędzy strefami musi być ograniczony do niezbędnych protokołów, portów, adresów, usług i kierunków komunikacji. Każde połączenie pomiędzy strefami musi mieć

uzasadnienie funkcjonalne, być opisane w dokumentacji projektowej, skonfigurowane zgodnie z zasadą minimalnych uprawnień i objęte monitorowaniem oraz logowaniem.

Niedopuszczalne jest pozostawienie niekontrolowanej komunikacji pomiędzy urządzeniami terenowymi, kamerami, sensorami, routerami, modemami, serwerami, usługami aplikacyjnymi, API, systemami zewnętrznymi i siecią administracyjną. Niedopuszczalne jest również stosowanie domyślnych, nieudokumentowanych albo tymczasowych reguł komunikacji jako rozwiązania produkcyjnego.

1.2.18.3. Bezpieczeństwo transmisji danych

Generalny Wykonawca zobowiązany jest zapewnić bezpieczeństwo transmisji danych pomiędzy lokalizacjami terenowymi, Centrum RIS, serwerownią zapasową, systemami zewnętrznymi i użytkownikami uprawnionymi.

Wymagania bezpieczeństwa transmisji obejmują co najmniej:

1) szyfrowanie transmisji w kanałach, w których przesyłane są dane administracyjne, uwierzytelniające, konfiguracyjne, pomiarowe, integracyjne, operatorskie, diagnostyczne lub dane wymagające ochrony;
2) stosowanie VPN albo innych równoważnych mechanizmów zabezpieczających dla transmisji przez sieci publiczne, operatorskie albo niezaufane;
3) stosowanie mechanizmów uwierzytelniania stron komunikacji;
4) zabezpieczenie dostępu do interfejsów administracyjnych urządzeń transmisyjnych;
5) separację ruchu zarządzającego od ruchu użytkowego, jeżeli pozwala na to architektura rozwiązania;
6) ochronę przed nieautoryzowaną zmianą konfiguracji urządzeń transmisyjnych;
7) ochronę przed nieautoryzowanym podłączeniem urządzeń do sieci;
8) monitorowanie dostępności, jakości i parametrów transmisji;
9) alarmowanie o utracie łączności, degradacji parametrów transmisji albo przełączeniu na tor zapasowy;
10) logowanie zdarzeń związanych z zestawieniem, przerwaniem, przełączeniem albo błędem transmisji.

W przypadku zastosowania redundantnych torów dostępowych Generalny Wykonawca zobowiązany jest zapewnić, aby mechanizmy przełączenia awaryjnego nie powodowały obejścia zasad bezpieczeństwa, segmentacji, kontroli dostępu, szyfrowania, monitoringu i logowania.

1.2.18.4. Kontrola dostępu logicznego

System RIS musi zapewniać kontrolę dostępu logicznego do wszystkich aplikacji, usług, interfejsów, API, paneli administracyjnych, konsol operatorskich, konsol serwisowych, urządzeń

sieciowych, urządzeń terenowych, rejestratorów, serwerów, maszyn wirtualnych, macierzy, systemów backupu i komponentów monitoringu technicznego.

Kontrola dostępu musi być oparta co najmniej na następujących zasadach:

1) zasada minimalnych uprawnień;
2) zasada rozdziału ról i odpowiedzialności;
3) zasada indywidualnych kont użytkowników;
4) zakaz współdzielenia kont imiennych;
5) ograniczenie stosowania kont wspólnych wyłącznie do przypadków technicznie uzasadnionych i zaakceptowanych przez Zamawiającego;
6) odrębne konta administracyjne i użytkowe;
7) rejestrowanie działań wykonywanych z użyciem kont uprzywilejowanych;
8) okresowy przegląd uprawnień;
9) odbieranie albo blokowanie uprawnień po ustaniu potrzeby dostępu;
10) dokumentowanie nadania, zmiany i odebrania uprawnień.

Generalny Wykonawca zobowiązany jest zaprojektować i wdrożyć model ról i uprawnień dla wszystkich dostarczanych aplikacji i usług cyfrowych. Model ten musi obejmować co najmniej role administratorów, operatorów, użytkowników utrzymaniowych, użytkowników technicznych, użytkowników integracyjnych, kont serwisowych oraz innych ról wymaganych dla prawidłowej eksploatacji systemu.

W przypadku API i integracji zewnętrznych dostęp musi być nadawany w sposób kontrolowany, z możliwością ograniczenia zakresu danych, funkcji, metod, częstotliwości wywołań, środowiska, adresów źródłowych, tokenów, certyfikatów albo innych parametrów technicznych właściwych dla przyjętego mechanizmu integracji.

1.2.18.5. Uwierzytelnianie i zarządzanie poświadczeniami

Generalny Wykonawca zobowiązany jest zapewnić bezpieczne mechanizmy uwierzytelniania użytkowników, administratorów, kont technicznych, usług, urządzeń i systemów zewnętrznych.

Wymaga się co najmniej:

1) stosowania indywidualnych kont dla użytkowników i administratorów;
2) stosowania silnych mechanizmów uwierzytelniania dla kont uprzywilejowanych;
3) stosowania wieloskładnikowego uwierzytelniania dla dostępu administracyjnego, zdalnego, serwisowego oraz dostępu do systemów krytycznych, jeżeli rozwiązanie techniczne na to pozwala;
4) wymuszenia zmiany haseł domyślnych przed przekazaniem systemu do eksploatacji;
5) zakazu stosowania domyślnych kont i haseł producenta w środowisku produkcyjnym;

6) bezpiecznego przechowywania haseł, kluczy, tokenów, certyfikatów i sekretów;
7) dokumentowania kont technicznych i serwisowych;
8) ograniczenia uprawnień kont technicznych wyłącznie do zakresu niezbędnego do realizacji ich funkcji;
9) możliwości rotacji haseł, kluczy, tokenów i certyfikatów;
10) niezwłocznej zmiany albo unieważnienia poświadczeń po ujawnieniu, podejrzeniu ujawnienia albo ustaniu potrzeby korzystania.

Wszelkie hasła, klucze, tokeny, certyfikaty, konta techniczne i konta serwisowe przekazywane Zamawiającemu muszą być przekazane w sposób bezpieczny, udokumentowany i umożliwiający ich późniejszą zmianę przez Zamawiającego. Niedopuszczalne jest pozostawienie mechanizmów dostępu znanych wyłącznie Generalnemu Wykonawcy, producentowi, podwykonawcy albo dostawcy urządzenia.

1.2.18.6. Zdalny dostęp administracyjny i serwisowy

Zdalny dostęp administracyjny i serwisowy do systemu RIS, jego komponentów, urządzeń terenowych, urządzeń sieciowych, serwerów, aplikacji, API, rejestratorów, kamer, sensorów, szaf teletechnicznych, UPS, listew zasilających, systemów monitoringu środowiskowego i innych zasobów może być realizowany wyłącznie w sposób kontrolowany, autoryzowany, szyfrowany, monitorowany i logowany.

Zdalny dostęp musi spełniać co najmniej następujące wymagania:

1) dostęp może być realizowany wyłącznie przez zatwierdzone przez Zamawiającego mechanizmy;
2) dostęp musi być ograniczony do uprawnionych osób, kont, adresów, urządzeń albo sieci;
3) dostęp musi być rejestrowany;
4) dostęp uprzywilejowany musi umożliwiać ustalenie osoby albo podmiotu wykonującego czynności;
5) dostęp musi być możliwy do czasowego włączenia, ograniczenia, zablokowania albo odebrania przez Zamawiającego;
6) dostęp serwisowy musi być wykorzystywany wyłącznie w zakresie niezbędnym do wykonania czynności serwisowych;
7) dostęp producenta, podwykonawcy albo dostawcy zewnętrznego wymaga zgody Zamawiającego i musi być objęty zasadami bezpieczeństwa obowiązującymi w projekcie;
8) niedopuszczalne jest stosowanie nieudokumentowanych tuneli, stałych połączeń serwisowych, zdalnych pulpitów, kont producenta albo kanałów komunikacji poza wiedzą Zamawiającego.

1.2.18.7. Bezpieczeństwo aplikacji, usług cyfrowych i API

Generalny Wykonawca zobowiązany jest zapewnić bezpieczeństwo aplikacji, portali, usług cyfrowych, interfejsów użytkownika, paneli administracyjnych, API i usług integracyjnych systemu RIS.

Wymagania obejmują co najmniej:

1) projektowanie aplikacji i API zgodnie z zasadami bezpiecznego cyklu życia oprogramowania;
2) stosowanie walidacji danych wejściowych i wyjściowych;
3) ochronę przed typowymi podatnościami aplikacyjnymi i podatnościami API;
4) ochronę przed nieautoryzowanym dostępem do danych i funkcji;
5) ochronę przed eskalacją uprawnień;
6) ochronę przed obejściem mechanizmów autoryzacji;
7) ochronę przed ujawnieniem danych konfiguracyjnych, diagnostycznych, systemowych i technicznych;
8) ograniczenie informacji ujawnianych w komunikatach błędów;
9) bezpieczną obsługę sesji, tokenów, kluczy i certyfikatów;
10) szyfrowanie transmisji;
11) rejestrowanie zdarzeń bezpieczeństwa;
12) monitorowanie dostępności i poprawności działania interfejsów;
13) wersjonowanie API;
14) dokumentowanie interfejsów, uprawnień, danych i sposobu obsługi błędów.

API systemu RIS musi umożliwiać kontrolowane udostępnianie danych dziedzinowych wyłącznie uprawnionym odbiorcom. Każdy odbiorca danych musi mieć przypisany zakres uprawnień odpowiadający jego roli, podstawie dostępu, zakresowi danych, celowi wykorzystania i wymaganiom Zamawiającego.

1.2.18.8. Bezpieczeństwo systemu CCTV

Podsystem CCTV musi zapewniać kontrolę dostępu, rozliczalność działań, ochronę prywatności, bezpieczeństwo transmisji obrazu, bezpieczeństwo rejestracji, bezpieczeństwo odtwarzania i bezpieczeństwo eksportu materiału wideo.

Wymagania bezpieczeństwa dla CCTV obejmują co najmniej:

1) zarządzanie użytkownikami, rolami i uprawnieniami;
2) ograniczenie dostępu do podglądu, odtwarzania, eksportu, konfiguracji, administracji, masek prywatności i ustawień kamer wyłącznie do osób uprawnionych;

3) rejestrowanie działań użytkowników i administratorów;
4) rejestrowanie eksportu materiału wideo, w tym zakresu eksportu, czasu, użytkownika, lokalizacji kamery i celu wykonania eksportu, jeżeli taki cel jest wymagany przez Zamawiającego;
5) zabezpieczenie materiału eksportowanego przed nieuprawnioną modyfikacją albo nieuprawnionym dostępem;
6) zapewnienie działania masek prywatności w podglądzie, nagraniu, odtwarzaniu i eksporcie;
7) monitorowanie dostępności kamer, rejestratorów, węzłów rejestracji, strumieni wideo, stacji klienckich i usług udostępniania obrazu;
8) alarmowanie o utracie kamery, utracie strumienia, utracie rejestracji, awarii węzła rejestracji, awarii dysków, przekroczeniu parametrów retencji albo awarii usług CCTV;
9) zapewnienie testów poprawności uprawnień, eksportu, retencji, masek prywatności, monitoringu technicznego i alarmów;
10) zapewnienie ciągłości rejestracji i możliwości odtworzenia nagrań zgodnie z wymaganiami PFU i Planu CCTV.

Niedopuszczalne jest udostępnienie funkcji administracyjnych CCTV użytkownikom, którzy nie posiadają odpowiednich uprawnień. Niedopuszczalne jest również pozostawienie kamer, rejestratorów albo usług CCTV z domyślnymi poświadczeniami, nieużywanymi usługami sieciowymi albo nieudokumentowaną konfiguracją.

1.2.18.9. Bezpieczeństwo systemu VHF/AIS/DGNSS

Podsystem VHF/AIS/DGNSS musi być objęty mechanizmami kontroli dostępu, monitoringu technicznego, alarmowania, rejestrowania zdarzeń, ochrony konfiguracji i nadzoru nad dostępnością usług.

Wymagania obejmują co najmniej:

1) kontrolę dostępu do konsol operatorskich i administracyjnych;
2) kontrolę dostępu do konfiguracji urządzeń stacji brzegowych;
3) kontrolę dostępu do urządzeń transmisyjnych i komponentów aplikacyjnych;
4) monitorowanie dostępności stacji brzegowych VHF, AIS i DGNSS;
5) monitorowanie stanu usług radiokomunikacyjnych i aplikacyjnych;
6) alarmowanie o awarii urządzenia, utracie łączności, utracie transmisji danych, błędach komponentów aplikacyjnych albo przekroczeniu parametrów pracy;
7) rejestrowanie zdarzeń związanych z pracą systemu, alarmami, awariami, czynnościami operatorskimi i administracyjnymi;

8) ochronę konfiguracji urządzeń i usług przed nieuprawnioną zmianą;
9) możliwość odtworzenia konfiguracji po awarii;
10) dokumentowanie konfiguracji, kont, połączeń, interfejsów, alarmów i procedur eksploatacyjnych.

Dostęp serwisowy do urządzeń VHF/AIS/DGNSS, konsol i komponentów aplikacyjnych musi być realizowany wyłącznie w trybie zaakceptowanym przez Zamawiającego, z zachowaniem zasad kontroli dostępu, logowania i rozliczalności.

1.2.18.10. Bezpieczeństwo czujników, sensorów i lokalnych komponentów akwizycji danych

Czujniki hydrologiczne, sensory meteorologiczne, lokalne sterowniki, konwertery, urządzenia buforujące, urządzenia komunikacyjne i komponenty przekazujące dane pomiarowe do Centrum RIS muszą być zabezpieczone przed nieuprawnionym dostępem, nieuprawnioną zmianą konfiguracji, utratą danych, modyfikacją danych, przerwą transmisji i utratą identyfikowalności danych.

Wymagania obejmują co najmniej:

1) kontrolę dostępu do konfiguracji urządzeń pomiarowych i lokalnych komponentów akwizycji danych;
2) ochronę interfejsów komunikacyjnych i serwisowych;
3) ograniczenie dostępu lokalnego i zdalnego wyłącznie do osób uprawnionych;
4) logowanie zmiany konfiguracji, zmiany parametrów pomiarowych, zmiany interwałów, zmiany korekt i zmiany ustawień transmisji;
5) oznaczanie danych identyfikatorem lokalizacji, urządzenia, czasu pomiaru i statusu jakości;
6) ochronę danych buforowanych lokalnie w czasie utraty łączności;
7) zachowanie rzeczywistego czasu pomiaru dla danych przekazywanych po wznowieniu transmisji;
8) monitorowanie dostępności urządzenia, opóźnień w przekazywaniu danych, braku nowych danych, błędów pomiarowych, błędów transmisji i utraty zasilania;
9) alarmowanie o zdarzeniach wpływających na wiarygodność, kompletność albo ciągłość danych pomiarowych;
10) możliwość odtworzenia konfiguracji urządzeń po awarii albo wymianie urządzenia.

1.2.18.11. Bezpieczeństwo szaf teletechnicznych i dostępu fizycznego

Szafy teletechniczne typu zewnętrznego oraz ich wyposażenie muszą być objęte kontrolą dostępu fizycznego, monitoringiem zdarzeń, alarmowaniem i logowaniem.

Wymagania obejmują co najmniej:

1) zabezpieczenie szafy przed dostępem osób nieuprawnionych;
2) zastosowanie zamków, systemu kontroli dostępu, czujników otwarcia drzwi i mechanizmów alarmowania zgodnie z wymaganiami PFU;
3) rejestrowanie zdarzeń otwarcia i zamknięcia szafy;
4) rejestrowanie zdarzeń nieautoryzowanego otwarcia albo próby dostępu;
5) monitorowanie temperatury, wilgotności, zasilania, UPS, listew zasilających, liczników energii, wentylacji i ogrzewania;
6) alarmowanie o przekroczeniu progów środowiskowych, utracie zasilania, pracy bateryjnej, awarii UPS, awarii wentylacji, awarii ogrzewania, utracie komunikacji z modułem monitorującym albo innym zdarzeniu mogącym wpływać na pracę urządzeń;
7) integrację zdarzeń i alarmów z systemem monitoringu technicznego zasobów RIS;
8) dokumentowanie konfiguracji urządzeń monitorujących, progów alarmowych, użytkowników, kart dostępowych i procedur serwisowych.

Generalny Wykonawca zobowiązany jest zapewnić, aby zdarzenia z kontroli dostępu do szaf teletechnicznych były możliwe do powiązania z lokalizacją, identyfikatorem szafy, czasem zdarzenia, rodzajem zdarzenia oraz użytkownikiem albo uprawnieniem technicznym, jeżeli system umożliwia taką identyfikację.

1.2.18.12. Monitoring techniczny i monitoring bezpieczeństwa

Generalny Wykonawca zobowiązany jest objąć monitoringiem technicznym i monitoringiem bezpieczeństwa wszystkie nowe, modernizowane, rekonfigurowane i integrowane komponenty systemu RIS, które mają wpływ na ciągłość działania, dostępność usług, bezpieczeństwo danych, bezpieczeństwo transmisji, bezpieczeństwo użytkowników, poprawność pomiarów, rejestrację obrazu, integracje zewnętrzne albo eksploatację lokalizacji terenowych.

Monitoring musi obejmować co najmniej:

1) dostępność urządzeń i usług;
2) stan interfejsów sieciowych;
3) stan łączy transmisyjnych;
4) stan usług aplikacyjnych;
5) stan API i integracji;
6) stan kamer, rejestratorów, strumieni wideo i usług CCTV;
7) stan urządzeń VHF/AIS/DGNSS;
8) stan czujników hydrologicznych i meteorologicznych;
9) stan lokalnych komponentów akwizycji danych;

10) stan urządzeń sieciowych i bezpieczeństwa;
11) stan serwerów, maszyn wirtualnych, macierzy, backupu i replikacji;
12) stan UPS, zasilania, listew zasilających, liczników energii i elementów środowiskowych;
13) zdarzenia kontroli dostępu;
14) zdarzenia bezpieczeństwa;
15) zdarzenia administracyjne;
16) błędy integracji i błędy wymiany danych;
17) wykorzystanie zasobów, jeżeli jest istotne dla oceny dostępności lub wydajności;
18) alarmy producentów urządzeń i systemów, jeżeli są udostępniane przez zastosowane rozwiązania.

Monitoring musi umożliwiać prezentację stanu zasobów w podziale na lokalizacje, podsystemy, grupy urządzeń, usługi, interfejsy, środowiska techniczne i kategorie alarmów. System monitorowania musi umożliwiać szybkie ustalenie czy zdarzenie dotyczy urządzenia terenowego, toru transmisyjnego, lokalizacji, usługi centralnej, aplikacji, API, integracji, zasilania, szafy, serwerowni, konta, uprawnień albo zdarzenia bezpieczeństwa.

Generalny Wykonawca zobowiązany jest zapewnić integrację monitoringu nowych i modernizowanych zasobów z istniejącym albo docelowym systemem monitorowania zasobów RIS. Jeżeli do realizacji tego celu wymagane są licencje, moduły, konektory, agenci, szablony monitorowania, profile urządzeń albo dodatkowa konfiguracja, muszą one zostać dostarczone i wdrożone przez Generalnego Wykonawcę w ramach wynagrodzenia.

1.2.18.13. Logowanie zdarzeń i rozliczalność działań

Wszystkie komponenty systemu RIS objęte przedmiotem zamówienia muszą generować, przechowywać i udostępniać logi w zakresie niezbędnym do zapewnienia rozliczalności działań, diagnostyki, obsługi incydentów, analizy przyczyn awarii, weryfikacji dostępności, potwierdzenia bezpieczeństwa i wykazania zgodności z wymaganiami PFU.

Logowanie musi obejmować co najmniej:

1) logowania i wylogowania użytkowników;
2) nieudane próby logowania;
3) blokady kont;
4) zmiany haseł i poświadczeń;
5) nadanie, zmianę i odebranie uprawnień;
6) działania administracyjne;
7) zmiany konfiguracji;
8) uruchomienie, zatrzymanie i restart usług;

9) błędy aplikacyjne;
10) błędy API i integracji;
11) wywołania API, w zakresie wymaganym dla audytu i bezpieczeństwa;
12) zdarzenia bezpieczeństwa;
13) zdarzenia kontroli dostępu;
14) zdarzenia monitoringu technicznego;
15) zdarzenia dotyczące transmisji danych;
16) zdarzenia dotyczące backupu, replikacji i odtwarzania;
17) eksport danych, raportów, nagrań albo materiałów wideo;
18) dostęp do danych wrażliwych, danych konfiguracyjnych albo funkcji administracyjnych;
19) operacje wykonywane na danych pomiarowych, w tym korekty i zatwierdzenia danych;
20) działania wykonywane przez konta techniczne, konta serwisowe i konta uprzywilejowane.

Logi muszą zawierać co najmniej czas zdarzenia, źródło zdarzenia, identyfikator użytkownika albo konta technicznego, identyfikator urządzenia albo usługi, kategorię zdarzenia, wynik operacji, adres źródłowy, jeżeli jest dostępny, oraz informacje umożliwiające analizę zdarzenia bez ujawniania w logach haseł, tokenów, kluczy, pełnych sekretów albo innych danych, których utrwalenie w logach byłoby niebezpieczne.

Czas systemowy wszystkich komponentów generujących logi musi być synchronizowany z wiarygodnym źródłem czasu wskazanym albo zaakceptowanym przez Zamawiającego. Synchronizacja czasu musi obejmować serwery, urządzenia sieciowe, urządzenia bezpieczeństwa, urządzenia terenowe, rejestratory, systemy CCTV, komponenty VHF/AIS/DGNSS, systemy monitoringu, aplikacje, API i inne komponenty, dla których czas zdarzenia ma znaczenie diagnostyczne, dowodowe albo eksploatacyjne.

Logi muszą być chronione przed nieuprawnionym dostępem, modyfikacją, usunięciem i nadpisaniem. Dostęp do logów musi być ograniczony do osób uprawnionych, a czynności wykonywane na logach muszą być rozliczalne.

Generalny Wykonawca zobowiązany jest zaprojektować i udokumentować zasady retencji logów dla poszczególnych kategorii zdarzeń. Retencja logów musi uwzględniać wymagania prawne, wymagania bezpieczeństwa, wymagania eksploatacyjne, możliwości techniczne systemu, potrzeby diagnostyczne oraz wymagania Zamawiającego.

1.2.18.14. Zarządzanie podatnościami, aktualizacjami i konfiguracją bezpieczeństwa

Generalny Wykonawca zobowiązany jest zapewnić bezpieczny cykl życia dostarczanych komponentów, obejmujący zarządzanie podatnościami, aktualizacjami, konfiguracją, poprawkami bezpieczeństwa, wersjami oprogramowania, firmware i zależnościami technologicznymi.

Wymagania obejmują co najmniej:

1) dostarczanie komponentów wspieranych przez producenta;
2) zakaz dostarczania komponentów niewspieranych, wycofanych z eksploatacji albo bez możliwości aktualizacji bezpieczeństwa, chyba że Zamawiający wyrazi na to pisemną zgodę;
3) wykonanie inwentaryzacji wersji oprogramowania, firmware, systemów operacyjnych, bibliotek, zależności i komponentów;
4) przygotowanie procedur aktualizacji oprogramowania i firmware;
5) weryfikację wpływu aktualizacji na działanie systemu;
6) testowanie aktualizacji przed wdrożeniem produkcyjnym, jeżeli charakter komponentu na to pozwala;
7) wykonywanie kopii konfiguracji przed zmianą;
8) możliwość odtworzenia konfiguracji po awarii albo błędnej aktualizacji;
9) dokumentowanie wszystkich zmian konfiguracyjnych;
10) przekazywanie Zamawiającemu informacji o podatnościach istotnych dla dostarczonych komponentów;
11) usuwanie albo ograniczanie podatności w okresie realizacji i gwarancji;
12) uwzględnienie wymagań Polityki Zarządzania Podatnościami opracowanej w ramach PFU.

Konfiguracja bezpieczeństwa musi obejmować co najmniej wyłączenie nieużywanych usług, zmianę domyślnych poświadczeń, ograniczenie dostępu administracyjnego, aktualizację oprogramowania, ustawienie bezpiecznych protokołów, konfigurację logowania, konfigurację monitoringu, ograniczenie dostępu do interfejsów serwisowych oraz dokumentowanie odstępstw od konfiguracji rekomendowanej.

1.2.18.15. Kopie zapasowe konfiguracji i odtwarzanie

Generalny Wykonawca zobowiązany jest zapewnić możliwość wykonania kopii zapasowych konfiguracji wszystkich istotnych komponentów systemu RIS, w szczególności urządzeń sieciowych, urządzeń bezpieczeństwa, routerów, przełączników, modemów, urządzeń VPN, rejestratorów, kamer, urządzeń VHF/AIS/DGNSS, lokalnych komponentów akwizycji danych, systemów monitoringu, aplikacji, API, baz danych, maszyn wirtualnych, usług integracyjnych i systemów zarządzania.

Wymagania obejmują co najmniej:

1) opracowanie procedur wykonywania kopii konfiguracji;
2) opracowanie procedur odtwarzania konfiguracji;

3) wykonanie kopii konfiguracji po uruchomieniu, po odbiorze oraz po każdej istotnej zmianie;
4) bezpieczne przechowywanie kopii konfiguracji;
5) ochronę kopii konfiguracji przed nieuprawnionym dostępem;
6) testowe odtworzenie wybranych konfiguracji w ramach testów odbiorowych albo testów utrzymaniowych;
7) przekazanie Zamawiającemu kopii konfiguracji w sposób uzgodniony i bezpieczny;
8) opisanie zależności pomiędzy konfiguracjami urządzeń, usług i systemów.

1.2.18.16. Ochrona danych i prywatności

Generalny Wykonawca zobowiązany jest zapewnić ochronę danych przetwarzanych w systemie RIS, w tym danych pomiarowych, danych lokalizacyjnych, danych użytkowników, danych technicznych, danych diagnostycznych, metadanych CCTV, logów, danych integracyjnych, danych konfiguracyjnych i danych udostępnianych przez API.

Wymagania obejmują co najmniej:

1) ograniczenie dostępu do danych do osób, systemów i usług uprawnionych;
2) szyfrowanie transmisji danych wymagających ochrony;
3) ochronę danych w API;
4) rozliczalność dostępu do danych;
5) kontrolę eksportu danych;
6) ochronę materiału wideo i metadanych CCTV;
7) stosowanie masek prywatności w systemie CCTV zgodnie z wymaganiami PFU i Planu CCTV;
8) minimalizację zakresu udostępnianych danych;
9) ochronę danych konfiguracyjnych, diagnostycznych i logów;
10) dokumentowanie kategorii danych, odbiorców danych, podstaw dostępu i mechanizmów ochrony.

1.2.18.17. Wymagania dotyczące testów bezpieczeństwa

Generalny Wykonawca zobowiązany jest przeprowadzić testy bezpieczeństwa wszystkich komponentów objętych przedmiotem zamówienia w zakresie adekwatnym do ich funkcji, ryzyka i sposobu eksploatacji.

Testy bezpieczeństwa muszą obejmować co najmniej:

1) weryfikację segmentacji sieci i reguł komunikacji;
2) weryfikację konfiguracji zapór, VPN, routerów i przełączników;

3) weryfikację mechanizmów uwierzytelniania i autoryzacji;
4) weryfikację modelu ról i uprawnień;
5) weryfikację braku domyślnych haseł i domyślnych kont;
6) weryfikację konfiguracji logowania;
7) weryfikację monitorowania i alarmowania;
8) weryfikację bezpieczeństwa API;
9) weryfikację bezpieczeństwa aplikacji webowych i paneli administracyjnych;
10) weryfikację bezpieczeństwa zdalnego dostępu;
11) weryfikację działania kontroli dostępu do CCTV;
12) weryfikację bezpieczeństwa eksportu danych i materiału wideo;
13) weryfikację działania masek prywatności w CCTV;
14) weryfikację bezpieczeństwa urządzeń terenowych, kamer, sensorów, routerów, modemów i sterowników;
15) weryfikację odtwarzania konfiguracji po awarii;
16) skanowanie podatności komponentów sieciowych, serwerowych, aplikacyjnych i urządzeń połączonych;
17) testy odporności na utratę łączności, utratę zasilania i awarie wybranych komponentów, w zakresie powiązanym z bezpieczeństwem i ciągłością działania.

Wyniki testów bezpieczeństwa muszą zostać udokumentowane raportami i protokołami. Raporty muszą zawierać co najmniej zakres testów, datę wykonania, środowisko, wykorzystane metody i narzędzia, wykaz badanych komponentów, wyniki, stwierdzone niezgodności, klasyfikację istotności, rekomendacje naprawcze, potwierdzenie usunięcia niezgodności oraz wynik ponownej weryfikacji.

Odbiór komponentu, usługi, aplikacji, API, integracji albo lokalizacji terenowej nie może nastąpić w przypadku występowania nieusuniętych podatności krytycznych albo wysokich, które wpływają na bezpieczeństwo, dostępność, integralność, poufność, rozliczalność albo możliwość eksploatacji systemu RIS, chyba że Zamawiający pisemnie zaakceptuje ryzyko i sposób jego ograniczenia.

1.2.18.18. Dokumentacja bezpieczeństwa

Generalny Wykonawca zobowiązany jest opracować i przekazać Zamawiającemu dokumentację bezpieczeństwa dla wszystkich komponentów objętych przedmiotem zamówienia.

Dokumentacja bezpieczeństwa musi obejmować co najmniej:

1) opis architektury bezpieczeństwa;
2) opis stref bezpieczeństwa i kanałów komunikacyjnych;

3) macierz komunikacji pomiędzy strefami;
4) wykaz reguł zapór sieciowych, VPN i mechanizmów separacji ruchu;
5) wykaz kont, ról, grup i uprawnień;
6) opis mechanizmów uwierzytelniania i autoryzacji;
7) opis kont technicznych i serwisowych;
8) zasady zarządzania poświadczeniami, kluczami, tokenami i certyfikatami;
9) opis konfiguracji bezpieczeństwa urządzeń i systemów;
10) opis mechanizmów logowania;
11) opis kategorii logów i zasad retencji;
12) opis integracji z monitoringiem technicznym i monitoringiem bezpieczeństwa;
13) opis progów alarmowych i reguł alarmowania;
14) opis zdalnego dostępu administracyjnego i serwisowego;
15) procedury nadawania, zmiany i odbierania dostępu;
16) procedury aktualizacji i zarządzania podatnościami;
17) procedury wykonywania i odtwarzania kopii konfiguracji;
18) procedury obsługi incydentów bezpieczeństwa w zakresie komponentów objętych zamówieniem;
19) procedury awaryjne dla utraty łączności, utraty zasilania, awarii urządzenia, awarii usługi, awarii integracji i naruszenia bezpieczeństwa;
20) raporty z testów bezpieczeństwa;
21) wykaz znanych ograniczeń, ryzyk i zaakceptowanych odstępstw.

Dokumentacja bezpieczeństwa musi być spójna z Dokumentacją Administratora, Dokumentacją Eksploatacyjną systemu RIS, Planem Ciągłości Działania BCP, Planem Odtworzenia po Awarii DRP, Polityką Zarządzania Podatnościami, dokumentacją monitoringu technicznego, dokumentacją integracji, dokumentacją API oraz dokumentacją powykonawczą.

1.2.18.19. Wymagania eksploatacyjne i gwarancyjne

W okresie realizacji przedmiotu zamówienia oraz w okresie gwarancji Generalny Wykonawca zobowiązany jest utrzymywać wymagany poziom bezpieczeństwa komponentów objętych jego odpowiedzialnością.

Obowiązek ten obejmuje co najmniej:

1) usuwanie błędów bezpieczeństwa;
2) usuwanie podatności dotyczących dostarczonych komponentów;
3) aktualizację konfiguracji bezpieczeństwa;

4) wsparcie Zamawiającego w analizie incydentów dotyczących dostarczonych komponentów;
5) aktualizację dokumentacji bezpieczeństwa po zmianach;
6) aktualizację konfiguracji monitoringu i alarmowania;
7) okresowe sprawdzenie poprawności logowania;
8) okresowe sprawdzenie kont, ról i uprawnień;
9) okresowe sprawdzenie kopii konfiguracji;
10) okresowe sprawdzenie możliwości odtworzenia konfiguracji;
11) przekazywanie Zamawiającemu informacji o istotnych podatnościach producentów;
12) wykonywanie czynności serwisowych w sposób kontrolowany, udokumentowany i bezpieczny.

Zmiana konfiguracji bezpieczeństwa, reguł komunikacji, kont uprzywilejowanych, interfejsów administracyjnych, mechanizmów zdalnego dostępu, integracji, API, systemów monitoringu albo mechanizmów logowania wymaga udokumentowania i akceptacji Zamawiającego, jeżeli może wpływać na bezpieczeństwo, dostępność, integralność, poufność albo rozliczalność systemu RIS.

1.2.18.20. Wymagania odbiorowe

Warunkiem odbioru komponentów objętych niniejszym rozdziałem jest potwierdzenie, że zostały one zaprojektowane, wykonane, skonfigurowane, zabezpieczone, przetestowane, udokumentowane i przekazane do eksploatacji zgodnie z wymaganiami PFU.

Odbiór musi obejmować co najmniej:

1) weryfikację architektury bezpieczeństwa;
2) weryfikację segmentacji i separacji ruchu;
3) weryfikację reguł komunikacji;
4) weryfikację szyfrowania transmisji;
5) weryfikację kontroli dostępu;
6) weryfikację kont, ról i uprawnień;
7) weryfikację braku domyślnych poświadczeń;
8) weryfikację konfiguracji zdalnego dostępu;
9) weryfikację monitoringu technicznego i monitoringu bezpieczeństwa;
10) weryfikację logowania zdarzeń;
11) weryfikację synchronizacji czasu;
12) weryfikację retencji i ochrony logów;

13) weryfikację bezpieczeństwa API i integracji;
14) weryfikację bezpieczeństwa CCTV;
15) weryfikację bezpieczeństwa VHF/AIS/DGNSS;
16) weryfikację bezpieczeństwa czujników, sensorów i komponentów akwizycji danych;
17) weryfikację bezpieczeństwa szaf teletechnicznych i kontroli dostępu fizycznego;
18) weryfikację kopii konfiguracji i możliwości odtworzenia;
19) weryfikację raportów z testów bezpieczeństwa;
20) weryfikację kompletności dokumentacji bezpieczeństwa.

Wszystkie stwierdzone niezgodności muszą zostać usunięte przed odbiorem, z wyjątkiem odstępstw pisemnie zaakceptowanych przez Zamawiającego wraz z określeniem ryzyka, sposobu jego ograniczenia, właściciela ryzyka i terminu usunięcia albo ponownej oceny.

1.2.19. Wymagania dotyczące dokumentacji systemu RIS

Wykonawca jest zobowiązany do wytworzenia i dostarczenia Zamawiającemu Dokumentacji związanej z realizacją Przedmiotu Zamówienia, która będzie podlegała odbiorom. Wykonawca ma obowiązek aktualizować dostarczoną i odebraną Dokumentację, tak, aby uwzględniała każdą zmianę dokonywaną w ramach Gwarancji (obowiązek ten nie dotyczy Dokumentacji Projektowej po wykonanym Wdrożeniu, gdyż rolę dokumentacyjną przejmie Dokumentacja Powykonawcza Systemu). Dostarczona dokumentacja musi być dostępna w elektronicznej w języku polskim oraz na żądanie Zamawiającego w wersji papierowej. Dopuszcza się język angielski w dokumentacji technicznej komponentów, które nie są dziełem Wykonawcy, a dokumentacja producenta w języku polskim nie jest dostępna.

Dokumenty powinny być przekazywane w wersji edytowalnej i w formacie uzgodnionym z Zamawiającym, z pełną historią wprowadzanych zmian (kto, kiedy, co) i oznaczeniem wersji.

UWAGA:

Przyjęta i odebrana przez Zamawiającego Dokumentacja oraz ustalenia szczegółowe poczynione przez Strony w trakcie prac projektowo-implementacyjnych będą punktem odniesienia do kontroli zgodności i poprawności wytwarzanych i Wdrażanych rozwiązań. W przypadku dostrzeżenia rozbieżności pomiędzy Opisem Przedmiotu Zamówienia, a przyjętym w Dokumentacji Projektowej założeniu, o sposobie jego realizacji będzie decydował Opis Przedmiotu Zamówienia zawarty w Umowie.

Dokumentacja musi się składać co najmniej z:

1.2.19.1. Dokumentacja Administratora

Dokumentacja Administratora ma zawierać:

1) instrukcje i procedury eksploatacyjne, tj. procedury postępowania podczas bieżącej eksploatacji, administracji i konserwacji Systemu (np. backup, odtworzenie, zarządzanie logami, zarządzanie użytkownikami i uprawnieniami, monitorowanie parametrów środowiska) niezbędne do zapewnienia prawidłowego działania Systemu i poprawnej jego aktualizacji,
2) opis instalacji i konfigurowania wszystkich Komponentów Systemu,
3) opis integracji z innymi Systemami Dziedzinowymi,
4) opis zarządzania zmianami w Systemie i sposób dokumentowania tych zmian,
5) hasła administratorskie dające maksymalne uprawnienia do Oprogramowania (hasła muszą być przekazane w bezpieczny sposób, w uzgodnieniu z Zamawiającym),
6) opis konfiguracji serwerów: opis konfiguracji systemu operacyjnego, spis usług działających na serwerze i ich konfiguracja oraz przydzielone im zasoby, etc.,
7) opis licencji Oprogramowania Standardowego, numery i klucze aktywacyjne oraz numery licencji, okres wsparcia producenta.

1.2.19.2. Dokumentacja Użytkownika

W ramach realizacji Przedmiotu Zamówienia Wykonawca opracuje, przekaże do Odbioru Zamawiającego oraz będzie aktualizował Dokumentację Użytkownika Systemu. Dokumentacja ma być sporządzona w języku polskim, w sposób zrozumiały dla docelowych użytkowników, z wykorzystaniem jasnych instrukcji krok po kroku, przykładów użycia, opisów komunikatów oraz materiału ilustracyjnego (np. zrzutów ekranów, schematów, oznaczeń elementów interfejsu).

Z uwagi na modułową budowę Systemu RIS Dokumentacja Użytkownika musi zostać przygotowana dwupoziomowo i obejmować:

1) Ogólny przewodnik użytkownika Systemu RIS – wspólny dokument nadrzędny, opisujący:
    a) przeznaczenie i ogólny zakres funkcjonalny Systemu RIS oraz jego Aplikacji / Komponentów,
    b) podstawowe zasady korzystania z Systemu RIS,
    c) sposób poruszania się po Systemie RIS i obsługi graficznego interfejsu użytkownika (GUI),
    d) zasady logowania, wylogowania, nawigacji, wyszukiwania, filtrowania, sortowania, pracy na listach, formularzach, załącznikach, powiadomieniach, komunikatach i raportach,
    e) wspólne elementy interfejsu, oznaczenia, ikony, przyciski, statusy, walidacje i komunikaty,

f) ogólne zasady bezpieczeństwa korzystania z Systemu RIS oraz postępowania w przypadku błędów i problemów użytkownika.

2) Dokumentacje Użytkownika dedykowane poszczególnym Aplikacjom/Komponentom – odrębne dokumenty, przygotowane odpowiednio do funkcji danej Aplikacji / Komponentu oraz grupy jego użytkowników, opisujące wyłącznie funkcjonalności właściwe dla danego obszaru, bez powielania treści zawartych w ogólnym przewodniku użytkownika Systemu RIS.

Dokumentacja Użytkownika dla każdej Aplikacji / Komponentu musi zawierać co najmniej:

a) cel i zakres wykorzystania danego Aplikacji / Komponentu,

b) wskazanie docelowych grup użytkowników oraz ich podstawowych uprawnień funkcjonalnych,

c) opis dostępnych funkcji, operacji i scenariuszy użytkowych,

d) instrukcje realizacji typowych czynności i obsługi spraw „krok po kroku”,

e) opis danych wejściowych, wymaganych pól, walidacji, wyników działań oraz możliwych stanów sprawy lub procesu,

f) opis komunikatów informacyjnych, ostrzeżeń i błędów wraz ze wskazaniem zalecanego sposobu postępowania użytkownika,

g) opis sytuacji wyjątkowych, najczęstszych problemów oraz sposobu ich zgłaszania,

h) odwołania do wspólnych zasad korzystania z Systemu RIS opisanych w ogólnym przewodniku.

Zamawiający wymaga, aby Dokumentacja Użytkownika:

a) była spójna ze stanem faktycznym Systemu RIS i odpowiadała wersji wdrożonej produkcyjnie,

b) była podzielona w sposób logiczny, przejrzysty i zgodny ze strukturą Systemu RIS,

c) umożliwiała samodzielne korzystanie z Systemu RIS przez użytkownika bez konieczności odwoływania się do wiedzy technicznej,

d) była dostarczona w wersji edytowalnej oraz PDF,

e) podlegała aktualizacji przy każdej zmianie funkcjonalnej, zmianie GUI lub zmianie sposobu obsługi Aplikacji / Komponentu.

Dokumentacja nie zostanie uznana za wykonaną należycie, jeżeli będzie miała charakter wyłącznie ogólny, nie będzie odpowiadała podziałowi Systemu na Aplikacje/Komponenty, będzie powielała te same treści w wielu dokumentach albo nie będzie dostosowana do potrzeb i kompetencji docelowych grup użytkowników.

1.2.19.3. Planu Ciągłości Działania BCP

Wykonawca opracuje i przekaże Zamawiającemu do Odbioru dokument „Plan Ciągłości Działania BCP” dla Systemu. Dokument ma określać zasady i procedury zapewniające utrzymanie albo wznowienie działania Systemu na akceptowalnym poziomie po wystąpieniu zakłócenia, w szczególności awarii, incydentu bezpieczeństwa, niedostępności komponentu, utraty danych, zakłócenia usług dostawcy lub niedostępności środowiska podstawowego pracy Systemu RIS.

Plan Ciągłości Działania BCP musi być opracowany dla rzeczywistej architektury i modelu eksploatacji Systemu oraz być spójny z dokumentacją bezpieczeństwa, procedurą obsługi incydentów, procedurą zarządzania zmianą, zasadami wykonywania kopii zapasowych, procedurami odtworzeniowymi oraz wymaganiami SLA. Plan musi bazować na wynikach analizy ryzyka oraz analizy wpływu na działalność (BIA), w tym identyfikować funkcje krytyczne, dopuszczalne czasy przerwy, wymagane poziomy odtworzenia oraz zależności techniczne i organizacyjne.

Dokument musi zawierać co najmniej:

1) cel, zakres, założenia oraz przesłanki stosowania Plan Ciągłości Działania BCP;
2) wskazanie ról, odpowiedzialności i ścieżek decyzyjnych, w tym osób uruchamiających Plan Ciągłości Działania BCP;
3) wykaz kontaktów operacyjnych i kanałów komunikacji wewnętrznej i zewnętrznej;
4) kryteria aktywacji, eskalacji, deaktywacji oraz przejścia do trybu odtworzeniowego;
5) identyfikację procesów, usług, komponentów i zasobów krytycznych dla działania Systemu;
6) kolejność odtwarzania usług, komponentów i środowisk;
7) cele odtworzeniowe dla poszczególnych elementów Systemu, w tym wymagane parametry RTO i RPO;
8) opis zasobów niezbędnych do utrzymania lub wznowienia działania, w tym kopii zapasowych, redundancji, środowisk zapasowych, narzędzi administracyjnych, dostępu uprzywilejowanego oraz personelu;
9) szczegółowe scenariusze postępowania dla co najmniej: awarii krytycznej, incydentu cyberbezpieczeństwa, utraty integralności danych, niedostępności środowiska podstawowego oraz konieczności pracy w trybie obejść tymczasowych;
10) procedury odtwarzania danych, weryfikacji poprawności odtworzenia, przywrócenia usług oraz powrotu z rozwiązań tymczasowych do docelowego trybu pracy;
11) zasady współpracy z dostawcami i poddostawcami, jeżeli ich usługi lub komponenty wpływają na ciągłość działania;
12) zasady dokumentowania przebiegu zdarzenia, decyzji, czasów odtworzenia, problemów oraz wniosków po zdarzeniu;
13) zasady testowania, przeglądu i aktualizacji Plan Ciągłości Działania BCP, w tym po zmianach architektury, zmianach ryzyka, testach i incydentach.

W ramach realizacji tego elementu przedmiotu zamówienia Wykonawca przekaże również: harmonogram testów Plan Ciągłości Działania BCP, scenariusze testowe, wzory protokołów z testów i aktywacji, wykaz wymaganych zasobów odtworzeniowych oraz rekomendacje organizacyjne i techniczne niezbędne do osiągnięcia wymaganych parametrów ciągłości

działania. Plan Ciągłości Działania BCP musi być dostarczony w wersji edytowalnej i PDF, podlegać akceptacji Zamawiającego oraz być aktualizowany przez Wykonawcę w okresie realizacji Umowy i Usługi Utrzymania.

1.2.19.4. Plan Odtworzenia po Awarii DRP

Wykonawca opracuje i przekaże Zamawiającemu do Odbioru dokument „Plan Odtworzenia po Awarii DRP” dla Systemu. Dokument ma mieć charakter techniczny i operacyjny oraz określać szczegółowe procedury odtworzenia zasobów Systemu i danych po wystąpieniu awarii krytycznej, w szczególności awarii infrastruktury, utraty dostępności środowiska podstawowego, utraty lub uszkodzenia danych, awarii komponentu krytycznego, incydentu bezpieczeństwa lub niedostępności usługi lub komponentu dostawcy zewnętrznego. Plan musi być opracowany dla rzeczywistej architektury i modelu eksploatacji Systemu oraz pozostawać spójny z Planem Ciągłości Działania, procedurą obsługi incydentów, procedurą wykonywania kopii zapasowych, procedurą zarządzania zmianą, dokumentacją techniczną i wymaganiami SLA.

Plan Odtworzenia po Awarii DRP musi zawierać co najmniej:

1) cel, zakres, założenia, odbiorców dokumentu i przesłanki jego stosowania;
2) role, odpowiedzialności i uprawnienia osób uczestniczących w odtworzeniu, w tym warunki uruchomienia i zakończenia realizacji Planu;
3) wykaz kontaktów operacyjnych, technicznych i decyzyjnych oraz kanałów komunikacji wewnętrznej i zewnętrznej;
4) identyfikację środowisk, usług, komponentów, danych i zależności krytycznych dla odtworzenia Systemu;
5) kolejność odtwarzania usług, środowisk, danych i komponentów oraz zależności pomiędzy nimi;
6) cele odtworzeniowe dla poszczególnych elementów Systemu, w tym wymagane parametry RTO i RPO;
7) opis wymaganych zasobów odtworzeniowych, w tym kopii zapasowych, redundancji, środowisk zapasowych, nośników, narzędzi administracyjnych, kont uprzywilejowanych, personelu i usług stron trzecich;
8) szczegółowe procedury techniczne odtworzenia infrastruktury, konfiguracji, aplikacji, integracji i danych, wraz z procedurami weryfikacji kompletności i poprawności odtworzenia;
9) procedury uruchomienia pracy w trybie zastępczym lub tymczasowym oraz procedury powrotu do docelowego środowiska pracy;
10) scenariusze postępowania co najmniej dla: utraty środowiska podstawowego, uszkodzenia bazy danych, awarii komponentu krytycznego, błędu aktualizacji, incydentu bezpieczeństwa skutkującego koniecznością odtworzenia oraz awarii po stronie dostawcy zależnego;

11) zasady dokumentowania przebiegu odtworzenia, w tym decyzji, wykonanych kroków, problemów, odstępstw i osiągniętych czasów odtworzenia;

12) zasady testowania, przeglądu i aktualizacji Planu, w tym po zmianach architektury, po testach oraz po incydentach i awariach.

W ramach realizacji tego elementu przedmiotu zamówienia Wykonawca przekaże również co najmniej: harmonogram testów DRP, scenariusze testowe, wzory protokołów z testów i aktywacji Plan Odtworzenia po Awarii DRP, listę zasobów i uprawnień niezbędnych do odtworzenia, a także rekomendacje techniczne i organizacyjne niezbędne do osiągnięcia wymaganych parametrów RTO i RPO. Plan musi być przekazany w wersji edytowalnej i PDF, podlegać akceptacji Zamawiającego oraz być utrzymywany i aktualizowany przez Wykonawcę przez okres realizacji Usługi Utrzymania.

1.2.19.5. Polityka Zarządzania Podatnościami

W ramach realizacji Przedmiotu Zamówienia Wykonawca opracuje, uzgodni z Zamawiającym, przekaże do Odbioru oraz przygotuje do wdrożenia dokument pod nazwą „Polityka Zarządzania Podatnościami”, dotyczący Systemu, jego środowisk, komponentów, interfejsów, usług ICT, produktów ICT, procesów ICT oraz elementów łańcucha dostaw wykorzystywanych do wytworzenia, wdrożenia, utrzymania i rozwoju Systemu. Dokument ma stanowić element dokumentacji bezpieczeństwa Systemu i pozostawać spójny co najmniej z dokumentacją bezpieczeństwa informacji, procedurą obsługi incydentów, procedurą zarządzania zmianą, procedurą utrzymania, zasadami współpracy z dostawcami oraz wymaganiami Umowy i SLA.

1.2.19.5.1. Wymagania ogólne dotyczące dokumentu

Dokument musi być opracowany dla rzeczywistej architektury, rzeczywistych procesów utrzymaniowych i rzeczywistego modelu świadczenia usług w ramach Systemu, a nie jako uniwersalny szablon producenta lub dostawcy.

Dokument musi być zgodny z obowiązkami Zamawiającego wynikającymi z UKSC, w szczególności w zakresie zbierania informacji o cyberzagrożeniach i podatnościach, zarządzania incydentami, usuwania podatności, bezpieczeństwa i ciągłości łańcucha dostaw, regularnych aktualizacji oprogramowania oraz dokumentowania środków bezpieczeństwa.

Dokument musi uwzględniać, że obsługa podatności może przejść w tryb incydentowy, a proces musi umożliwiać Zamawiającemu dochowanie ustawowych terminów zgłaszania incydentów poważnych, w tym wczesnego ostrzeżenia w terminie do 24 godzin i zgłoszenia incydentu poważnego w terminie do 72 godzin od wykrycia, a także przygotowania sprawozdania końcowego.

Dokument musi być spójny z podejściem opartym na ryzyku i uwzględniać bezpieczeństwo łańcucha dostaw, bezpieczeństwo w procesie nabywania, rozwoju i utrzymania systemów oraz postępowanie w przypadku podatności i ich ujawniania, zgodnie z kierunkiem wynikającym z dyrektywy NIS2.

1.2.19.5.2. Minimalna wymagana zawartość dokumentu

Dokument „Polityka Zarządzania Podatnościami” musi zawierać co najmniej następujące rozdziały i elementy:

1) Cel, zakres i status dokumentu, w tym wskazanie właściciela dokumentu, właściciela procesu, daty obowiązywania, zasad przeglądu i aktualizacji oraz relacji do innych dokumentów bezpieczeństwa i utrzymania.
2) Podstawy formalne i odniesienia, w tym odniesienie do Umowy, SWZ, umowy, SLA, dokumentacji bezpieczeństwa Systemu, procedury obsługi incydentów, procedury zarządzania zmianą, procedury utrzymania, wymagań dla dostawców oraz przyjętych norm, dobrych praktyk i wytycznych.
3) Słownik pojęć i definicji, obejmujący co najmniej: podatność, podatność potencjalna, podatność potwierdzona, podatność krytyczna, wysoka, średnia i niska, aktywo, komponent krytyczny, ekspozycja, poprawka bezpieczeństwa, obejście tymczasowe, remediacja, akceptacja ryzyka, wyjątek, właściciel ryzyka, incydent bezpieczeństwa, zgłoszenie zewnętrzne, skoordynowane ujawnianie podatności.
4) Zakres przedmiotowy polityki, obejmujący co najmniej: Oprogramowanie Aplikacyjne, systemy operacyjne, bazy danych, middleware, biblioteki i zależności, komponenty open source, kontenery, obrazy, usługi chmurowe, urządzenia sieciowe, urządzenia bezpieczeństwa, interfejsy API, mechanizmy CI/CD, konfiguracje bezpieczeństwa, integracje zewnętrzne oraz komponenty i usługi pochodzące od dostawców i poddostawców.
5) Role, odpowiedzialności i ścieżki eskalacji, obejmujące co najmniej: właściciela procesu, koordynatora ds. cyberbezpieczeństwa, zespół utrzymania, zespół deweloperski, administratorów, właścicieli biznesowych, osoby zatwierdzające wyjątki i akceptację ryzyka, dostawców, poddostawców oraz punkty kontaktowe do współpracy z Zamawiającym.
6) Źródła informacji o podatnościach oraz sposób ich monitorowania, obejmujące co najmniej: biuletyny producentów, bazy i repozytoria podatności, komunikaty dostawców, wyniki skanów, wyniki audytów i testów bezpieczeństwa, zgłoszenia użytkowników, zgłoszenia badaczy bezpieczeństwa, informacje od CSIRT/CERT, informacje z narzędzi monitorowania bezpieczeństwa oraz inne uzgodnione źródła threat intelligence.
7) Zasady przyjmowania i rejestrowania zgłoszeń, w tym kanały zgłoszeń, minimalny zakres danych w zgłoszeniu, sposób potwierdzania przyjęcia, reguły nadawania numeru sprawy, prowadzenia śladu audytowego, oceny wiarygodności zgłaszającego i obowiązek prowadzenia rejestru podatności.
8) Opis procesu zarządzania podatnościami, obejmujący co najmniej etapy: przygotowanie, przyjęcie zgłoszenia, weryfikację, analizę wpływu, klasyfikację, opracowanie działań korygujących lub kompensacyjnych, wdrożenie, testy, potwierdzenie usunięcia, działania po wdrożeniu oraz zamknięcie sprawy.
9) Metodykę oceny i klasyfikacji podatności, uwzględniającą co najmniej: techniczną wagę podatności, krytyczność aktywa, ekspozycję na Internet, poziom uprzywilejowania, dostępność exploitu, możliwość wykorzystania w łańcuchu ataku, wpływ na poufność, integralność, dostępność i autentyczność, wpływ na świadczenie usługi, wpływ na inne podmioty, wpływ regulacyjny oraz zależności w łańcuchu dostaw.
10) Czasy reakcji i terminy remediacji, określone co najmniej dla: potwierdzenia zgłoszenia, wstępnej klasyfikacji, analizy wpływu, przedstawienia planu działań, wdrożenia obejścia tymczasowego, wdrożenia poprawki, potwierdzenia skuteczności usunięcia oraz

zamknięcia sprawy. Dokument musi przewidywać odrębne, zaostrzone terminy dla podatności krytycznych i wysokich.

11) Zasady testowania, wdrażania i wycofywania poprawek bezpieczeństwa, w tym: testy przedwdrożeniowe, zasady wdrożeń awaryjnych, weryfikację integralności źródła poprawki, warunki rollback, dokumentowanie wpływu na produkcję oraz powiązanie z procesem zarządzania zmianą.
12) Zasady postępowania w przypadku braku poprawki albo niemożności jej wdrożenia, w tym: katalog środków kompensacyjnych, tryb czasowej akceptacji ryzyka, poziom wymaganych zgód, maksymalny okres obowiązywania wyjątku, częstotliwość przeglądu wyjątku oraz obowiązek dokumentowania ryzyka rezydualnego.
13) Powiązanie procesu zarządzania podatnościami z obsługą incydentów, w tym wskazanie, kiedy podatność jest traktowana jako zdarzenie bezpieczeństwa lub incydent, kiedy następuje eskalacja do procedury incydentowej oraz jakie dane muszą zostać przekazane, aby umożliwić Zamawiającemu wykonanie obowiązków ustawowych wobec właściwego CSIRT.
14) Zasady skoordynowanego ujawniania podatności, jeżeli mają zastosowanie do Systemu lub jego komponentów, obejmujące co najmniej: kanał zgłoszeń od badaczy bezpieczeństwa, zasady poufności, sposób komunikacji ze zgłaszającym, zasady publikacji informacji po usunięciu lub ograniczeniu ryzyka oraz wymagania co do publicznego punktu kontaktowego.
15) Wymagania wobec dostawców i poddostawców, w tym obowiązek przekazywania informacji o podatnościach i biuletynach bezpieczeństwa, obowiązek współpracy przy analizie wpływu i remediacji, wymagania dla EOL/EOS, obowiązek zgłaszania zmian wpływających na bezpieczeństwo oraz zasady oceny ryzyka związanego z dostawcą.
16) Narzędzia, rejestry i dowody wykonania, w tym obowiązek prowadzenia co najmniej: rejestru podatności, rejestru wyjątków, rejestru działań korygujących, rejestru decyzji o akceptacji ryzyka, historii wdrożeń poprawek, raportów ze skanów, wyników testów, zapisów z systemu zgłoszeniowego oraz innych artefaktów potwierdzających realizację procesu.
17) Wskaźniki, raportowanie i przeglądy, w tym co najmniej: liczbę podatności według kategorii, średni czas klasyfikacji, średni czas remediacji, odsetek podatności usuniętych w terminie, liczbę wyjątków, liczbę aktywów bez aktualnych danych o podatnościach, stan zaległych poprawek oraz informacje o podatnościach związanych z łańcuchem dostaw. Dokument powinien określać częstotliwość raportowania do Zamawiającego i częstotliwość przeglądu samej polityki.
18) Zasady wersjonowania, zatwierdzania, dystrybucji i retencji dokumentu, w tym oznaczanie kolejnych wersji, identyfikowanie zmian, ograniczenie dostępu do osób upoważnionych oraz okres przechowywania dokumentacji.

1.2.19.5.3. Wymagane załączniki do dokumentu

Wraz z dokumentem Wykonawca przekaże co najmniej następujące załączniki operacyjne:

1) wzór rejestru podatności,
2) wzór rejestru wyjątków i akceptacji ryzyka,
3) wzór planu remediacji,
4) wzór raportu okresowego z zarządzania podatnościami,
5) matrycę ról i odpowiedzialności,
6) wykaz źródeł monitorowania podatności,

7) wzór zgłoszenia podatności od podmiotu zewnętrznego,
8) wzór decyzji o czasowym zastosowaniu środków kompensacyjnych,
9) opis minimalnego zestawu dowodów potwierdzających wykonanie procesu.

1.2.19.5.4. Wymagania eksploatacyjne po odbiorze

Wykonawca zapewni w okresie świadczenia Gwarancji na System RIS aktualizację dokumentu w przypadku zmian architektury Systemu, zmian w łańcuchu dostaw, zmian modelu utrzymania, ujawnienia nowych klas podatności, wystąpienia incydentu wpływającego na proces obsługi podatności albo zmian przepisów lub wymagań bezpieczeństwa mających zastosowanie do Systemu. Taki obowiązek pozostaje zgodny z wymaganiem aktualizacji środków bezpieczeństwa, dokumentacji i praktyk zarządzania ryzykiem adekwatnie do zagrożeń i zmian w środowisku systemowym.

1.2.19.5.5. Wymagania odbiorowe i kryteria akceptacji dokumentu Polityka Zarządzania Podatnościami

Podstawy formalne i odniesienia, w tym odniesienie do PFU, SWZ, Umowy, parametrów SLA określonych w Umowie, dokumentacji bezpieczeństwa systemu RIS, procedury obsługi incydentów, procedury zarządzania zmianą, procedury utrzymania, wymagań dla dostawców oraz przyjętych norm, dobrych praktyk i wytycznych.

Zamawiający ma prawo zgłosić uwagi, żądać uzupełnień, korekt i doprecyzowań, a Wykonawca jest zobowiązany do ich uwzględnienia w terminie wskazanym przez Zamawiającego. Wersje dokumentu muszą umożliwiać identyfikację zmian.

Dokument nie zostanie uznany za wykonany należycie, jeżeli:

a) ma charakter ogólny i nie odnosi się do rzeczywistego Systemu,
b) nie zawiera mierzalnych terminów i odpowiedzialności,
c) nie opisuje relacji z obsługą incydentów i zarządzaniem zmianą,
d) nie obejmuje łańcucha dostaw,
e) nie określa rejestrów, dowodów wykonania i zasad raportowania,
f) nie określa zasad wersjonowania, aktualizacji i retencji,
g) nie zapewnia Zamawiającemu możliwości realizacji obowiązków ustawowych w zakresie podatności i incydentów.

Wykonawca przekaże dokument w wersji edytowalnej oraz w formacie PDF, wraz z metryką dokumentu, historią zmian i listą uwag uwzględnionych po uzgodnieniach z Zamawiającym.

1.2.19.6. Dokumentacja eksploatacyjna systemu RIS

1.2.19.6.1. Obowiązek opracowania dokumentu

Generalny Wykonawca opracuje i przekaże Zamawiającemu dokument pod nazwą „Dokumentacja eksploatacyjna systemu RIS”.

Dokument musi zostać przekazany Zamawiającemu do weryfikacji i akceptacji przed przystąpieniem do Odbioru Końcowego. Przekazanie Zamawiającemu zaakceptowanej „Dokumentacji eksploatacyjnej systemu RIS” stanowi warunek przystąpienia do Odbioru Końcowego.

Brak dokumentu, brak kompletności dokumentu, brak zgodności dokumentu z rzeczywistym zakresem wdrożenia albo brak akceptacji Zamawiającego stanowi podstawę do odmowy rozpoczęcia procedury Odbioru Końcowego albo do wstrzymania tej procedury do czasu usunięcia braków.

1.2.19.6.2. Cel dokumentu

„Dokumentacja eksploatacyjna systemu RIS” będzie podstawowym dokumentem utrzymaniowym dla zasobów systemu RIS objętych realizacją przedmiotu zamówienia. Dokument musi zapewniać Zamawiającemu możliwość prawidłowego, bezpiecznego i powtarzalnego utrzymania systemu RIS po zakończeniu wdrożenia, w tym możliwość:

1) identyfikacji zasobów objętych dokumentacją;
2) ustalenia zasad bieżącej eksploatacji systemu;
3) ustalenia sposobu postępowania przy typowych czynnościach operacyjnych;
4) ustalenia sposobu zapewnienia niezawodności działania systemu;
5) ustalenia sposobu prowadzenia testów okresowych;
6) ustalenia sposobu prowadzenia czynności konserwacyjnych;
7) ustalenia zasad wykonywania kopii zapasowych i odtwarzania konfiguracji albo danych;
8) ustalenia zasad reagowania na awarie, alarmy, utratę łączności, utratę zasilania, utratę dostępności usługi albo degradację parametrów pracy;
9) ustalenia zasad korzystania z dokumentów powiązanych, instrukcji producentów, procedur technicznych i dokumentacji powykonawczej;
10) ustalenia granicy odpowiedzialności Generalnego Wykonawcy w stosunku do zasobów istniejących, jeżeli zostały wykorzystane, zmodernizowane, skonfigurowane, zintegrowane albo objęte zakresem wdrożenia.

Dokument nie może mieć charakteru ogólnego opisu marketingowego ani wyłącznie zestawienia dostarczonych produktów. Dokument musi mieć charakter praktyczny, eksploatacyjny i instruktażowy.

1.2.19.6.3. Zakres zasobów objętych dokumentacją

„Dokumentacja eksploatacyjna systemu RIS” musi obejmować zasoby, komponenty, podsystemy, konfiguracje, aplikacje, instalacje, interfejsy i usługi, które zostały przez Generalnego Wykonawcę:

1) dostarczone;
2) wykonane;
3) zainstalowane;
4) skonfigurowane;
5) uruchomione;
6) zmodernizowane;
7) rozbudowane;
8) wymienione;
9) zintegrowane;
10) objęte odpowiedzialnością gwarancyjną, serwisową, utrzymaniową albo eksploatacyjną w ramach realizacji przedmiotu zamówienia.

Dokumentacja nie musi obejmować zasobów dostarczonych w ramach wcześniejszych etapów budowy lub rozbudowy systemu RIS, jeżeli Generalny Wykonawca nie dokonał w nich ingerencji, nie wykorzystał ich jako elementu własnego rozwiązania, nie objął ich odpowiedzialnością i nie wprowadził zmian wpływających na ich eksploatację.

Jeżeli rozwiązanie Generalnego Wykonawcy współpracuje z zasobami istniejącymi, dokumentacja musi jednoznacznie wskazywać:

1) zasoby istniejące wykorzystywane przez rozwiązanie Generalnego Wykonawcę;
2) zakres powiązania tych zasobów z rozwiązaniem wdrożonym w ramach zamówienia;
3) zasoby istniejące objęte dokumentacją w całości;
4) zasoby istniejące objęte dokumentacją wyłącznie w zakresie dokonanej ingerencji;
5) zasoby istniejące wyłączone z dokumentacji eksploatacyjnej Generalnego Wykonawcy;
6) uzasadnienie przyjętego rozgraniczenia.

Ostateczny zakres dokumentacji musi wynikać z przyjętego i zatwierdzonego sposobu realizacji przedmiotu zamówienia, dokumentacji projektowej, dokumentacji powykonawczej, konfiguracji końcowej systemu oraz zakresu odpowiedzialności Generalnego Wykonawcy.

1.2.19.6.4. Wymagania ogólne dotyczące dokumentu

„Dokumentacja eksploatacyjna systemu RIS” musi być opracowana w sposób kompletny, spójny, przejrzysty i możliwy do praktycznego wykorzystania przez Zamawiającego oraz wskazany personel eksploatacyjny.

Dokument musi zawierać co najmniej:

1) stronę tytułową;
2) metrykę dokumentu;
3) historię zmian;
4) spis treści;
5) wykaz stosowanych skrótów i pojęć;
6) cel i zakres dokumentu;
7) opis zasad korzystania z dokumentu;
8) wykaz dokumentów powiązanych;
9) wykaz zasobów objętych dokumentacją;
10) wykaz lokalizacji objętych dokumentacją;
11) opis podsystemów, komponentów, usług i instalacji objętych dokumentacją;
12) opis procedur eksploatacyjnych;
13) opis metod zapewnienia wymaganego poziomu niezawodności;
14) opis procedur okresowych testów;
15) opis procedur konserwacji;
16) opis procedur awaryjnych;
17) opis zasad wykonywania kopii zapasowych, odtwarzania konfiguracji i odtwarzania danych, jeżeli dotyczy;
18) opis zasad aktualizacji oprogramowania i oprogramowania układowego, jeżeli dotyczy;
19) opis zasad monitorowania działania komponentów, usług i interfejsów;
20) opis zasad dokumentowania czynności eksploatacyjnych;
21) wymagania dotyczące kwalifikacji osób wykonujących czynności eksploatacyjne;
22) wykaz czynności wymagających udziału producenta, autoryzowanego serwisu albo osoby posiadającej wymagane uprawnienia;
23) załączniki zawierające zestawienia, formularze, protokoły, listy kontrolne i odwołania do dokumentów szczegółowych.

Dokument musi być zgodny z dokumentacją powykonawczą, dokumentacją instalacji i konfiguracji, dokumentacją producentów, instrukcjami obsługi, dokumentacją licencyjną, warunkami gwarancji oraz zatwierdzonym stanem końcowym systemu RIS.

1.2.19.6.5. Wykaz dokumentów powiązanych

Generalny Wykonawca zamieści w „Dokumentacji eksploatacyjnej systemu RIS” wykaz dokumentów powiązanych, z których korzystanie jest niezbędne albo przydatne przy eksploatacji systemu.

Wykaz musi zawierać co najmniej:

1) nazwę dokumentu;
2) wersję dokumentu;
3) datę dokumentu;
4) autora albo dostawcę dokumentu;
5) zakres odwołania;
6) komponent, podsystem albo usługę, której dokument dotyczy;
7) lokalizację dokumentu w repozytorium dokumentacji;
8) informację czy dokument stanowi załącznik, dokument nadrzędny, dokument źródłowy, instrukcję producenta, procedurę techniczną czy dokument pomocniczy.

Wykaz dokumentów powiązanych musi obejmować w szczególności dokumentację powykonawczą, dokumentację instalacji i konfiguracji, instrukcje obsługi, instrukcje administratora, instrukcje producentów, procedury kopii zapasowych, procedury odtwarzania, procedury testowania, dokumentację licencyjną, dokumenty gwarancyjne oraz dokumentację narzędzi monitorujących i administracyjnych.

1.2.19.6.6. Struktura opisu podsystemów i komponentów

Dla każdego podsystemu, komponentu, usługi, instalacji albo grupy zasobów objętych dokumentacją Generalny Wykonawca zastosuje jednolity układ opisu obejmujący co najmniej:

1) nazwę podsystemu, komponentu albo usługi;
2) funkcję pełnioną w systemie RIS;
3) lokalizację albo lokalizacje występowania;
4) powiązania z innymi podsystemami, komponentami, usługami, interfejsami albo zasobami istniejącymi;

5) podstawowe parametry eksploatacyjne;
6) tryb pracy;
7) wymagania dotyczące bieżącego nadzoru;
8) procedury operacyjne;
9) metody zapewnienia wymaganego poziomu niezawodności;
10) procedury okresowych testów;
11) procedury konserwacji;
12) procedury awaryjne;
13) zasady wykonywania kopii zapasowych albo odtwarzania konfiguracji, jeżeli dotyczy;
14) zasady aktualizacji oprogramowania, oprogramowania układowego albo konfiguracji, jeżeli dotyczy;
15) typowe objawy awarii i zalecane czynności diagnostyczne;
16) wykaz czynności wykonywanych przez Zamawiającego;
17) wykaz czynności wykonywanych wyłącznie przez Generalnego Wykonawcę, producenta, autoryzowany serwis albo osobę posiadającą wymagane uprawnienia;
18) dokumenty powiązane i instrukcje szczegółowe.

1.2.19.6.7. Procedury operacyjne

Procedury operacyjne muszą opisywać czynności wykonywane w normalnym trybie pracy systemu.

Zakres procedur operacyjnych musi być dostosowany do charakteru danego podsystemu albo komponentu i obejmować w szczególności:

1) sposób uruchomienia komponentu albo usługi;
2) sposób zatrzymania komponentu albo usługi;
3) sposób bezpiecznego restartu;
4) sposób logowania do interfejsu administracyjnego albo operatorskiego;
5) sposób sprawdzenia stanu pracy;
6) sposób sprawdzenia dostępności usługi;
7) sposób sprawdzenia podstawowych parametrów;
8) sposób odczytu alarmów, zdarzeń i komunikatów;
9) sposób wykonania podstawowych czynności eksploatacyjnych;

10) sposób potwierdzenia prawidłowego działania po wykonaniu czynności;

11) ograniczenia eksploatacyjne;

12) czynności zabronione albo wymagające wcześniejszej zgody Zamawiającego.

Procedury muszą być opisane w sposób sekwencyjny, z podaniem warunków wejściowych, wymaganych uprawnień, przebiegu czynności, oczekiwanego rezultatu i sposobu weryfikacji rezultatu.

1.2.19.6.8. Metody zapewnienia wymaganego poziomu niezawodności

Dla każdego istotnego podsystemu, komponentu albo usługi Generalny Wykonawca opisze metody zapewnienia wymaganego poziomu niezawodności.

Opis musi obejmować, adekwatnie do charakteru rozwiązania:

1) zastosowane mechanizmy redundancji;

2) zastosowane mechanizmy przełączenia awaryjnego;

3) zastosowane mechanizmy automatycznego odtwarzania pracy;

4) zastosowane mechanizmy buforowania danych;

5) zastosowane mechanizmy synchronizacji danych;

6) zastosowane mechanizmy monitoringu technicznego;

7) zastosowane mechanizmy alarmowania;

8) zależności od zasilania, transmisji danych, usług sieciowych, baz danych, systemów centralnych albo zasobów terenowych;

9) elementy krytyczne dla ciągłości działania;

10) dopuszczalne skutki awarii pojedynczego komponentu;

11) wymagane działania po awarii;

12) wymagane działania po przywróceniu działania komponentu;

13) minimalne czynności kontrolne potwierdzające przywrócenie prawidłowej pracy.

Jeżeli dany komponent nie posiada mechanizmów redundancji albo przełączenia awaryjnego, dokumentacja musi to jednoznacznie wskazywać oraz opisywać sposób postępowania w przypadku jego niedostępności.

1.2.19.6.9. Procedury okresowych testów

Dokumentacja musi określać procedury testów okresowych wykonywanych w celu potwierdzenia sprawności systemu, podsystemu, komponentu, interfejsu, mechanizmu awaryjnego albo instalacji.

Dla każdej procedury testowej Generalny Wykonawca wskaże co najmniej:

1) nazwę testu;
2) cel testu;
3) zakres testu;
4) komponenty objęte testem;
5) wymaganą częstotliwość;
6) wymagane uprawnienia personelu;
7) warunki rozpoczęcia testu;
8) wymagane przygotowanie systemu;
9) czynności testowe krok po kroku;
10) oczekiwany wynik testu;
11) sposób potwierdzenia wyniku;
12) sposób udokumentowania testu;
13) sposób przywrócenia normalnego trybu pracy;
14) sposób postępowania w przypadku wyniku negatywnego;
15) wpływ testu na ciągłość działania systemu RIS.

Procedury testowe muszą obejmować w szczególności testy mechanizmów redundancji, testy przełączenia awaryjnego, testy dostępności usług, testy łączności, testy odtwarzania konfiguracji, testy odtwarzania danych, testy rejestracji, testy alarmowania, testy zasilania awaryjnego oraz testy komponentów pomiarowych, jeżeli występują w rozwiązaniu.

1.2.19.6.10. Procedury konserwacji

Dokumentacja musi określać procedury konserwacji dla zasobów objętych dokumentacją.

Procedury konserwacji muszą obejmować co najmniej:

1) zakres czynności konserwacyjnych;
2) częstotliwość ich wykonywania;

3) wymagane narzędzia, materiały i części eksploatacyjne;
4) wymagane kwalifikacje personelu;
5) wymagania BHP;
6) wpływ czynności na dostępność systemu;
7) sposób przygotowania komponentu do konserwacji;
8) sposób wykonania czynności;
9) sposób potwierdzenia prawidłowego działania po konserwacji;
10) sposób udokumentowania wykonanych czynności;
11) czynności wymagające udziału producenta, autoryzowanego serwisu albo specjalistycznej firmy.

W odniesieniu do komponentów, dla których producent nie wymaga specjalnych czynności konserwacyjnych, dokumentacja musi zawierać jednoznaczną informację o braku takich wymagań oraz wskazywać minimalne czynności kontrolne, które muszą być wykonywane w ramach eksploatacji.

1.2.19.6.11. Procedury awaryjne i diagnostyczne

„Dokumentacja eksploatacyjna systemu RIS” musi zawierać procedury postępowania w przypadku awarii, utraty dostępności, alarmu, błędu konfiguracji, utraty łączności, utraty zasilania, utraty danych, degradacji parametrów pracy albo nieprawidłowego działania usługi.

Procedury awaryjne muszą obejmować co najmniej:

1) opis typowych objawów awarii;
2) możliwe przyczyny;
3) sposób wstępnej diagnostyki;
4) czynności możliwe do wykonania przez Zamawiającego;
5) czynności zastrzeżone dla Generalnego Wykonawcy, producenta albo autoryzowanego serwisu;
6) sposób eskalacji;
7) minimalny zakres informacji przekazywany w zgłoszeniu serwisowym;
8) sposób zabezpieczenia danych, konfiguracji i materiału dowodowego;
9) sposób potwierdzenia usunięcia awarii;
10) sposób udokumentowania zdarzenia.

Procedury awaryjne muszą być opisane tak, aby umożliwiały szybkie rozpoznanie problemu i ograniczenie skutków awarii bez ryzyka pogorszenia stanu systemu.

1.2.19.6.12. Kopie zapasowe i odtwarzanie

Jeżeli w ramach rozwiązania występują dane, konfiguracje, bazy danych, maszyny wirtualne, pliki konfiguracyjne, nagrania, rejestry zdarzeń albo inne zasoby wymagające zabezpieczenia, dokumentacja musi zawierać zasady wykonywania kopii zapasowych i odtwarzania.

Opis musi obejmować co najmniej:

1) zakres danych i konfiguracji objętych kopiami zapasowymi;
2) częstotliwość wykonywania kopii;
3) miejsce przechowywania kopii;
4) okres retencji;
5) osoby albo role uprawnione do wykonywania kopii;
6) osoby albo role uprawnione do odtwarzania;
7) procedurę wykonania kopii;
8) procedurę weryfikacji poprawności kopii;
9) procedurę odtworzenia;
10) procedurę testowego odtworzenia;
11) sposób dokumentowania wykonania kopii i odtworzenia;
12) zależności od innych systemów, usług albo nośników.

Przed każdą zmianą konfiguracji, aktualizacją oprogramowania, aktualizacją oprogramowania układowego albo czynnością mogącą wpływać na stabilność działania komponentu musi zostać wykonana kopia bezpieczeństwa konfiguracji, danych albo innego właściwego zasobu, jeżeli jest to technicznie uzasadnione.

1.2.19.6.13. Aktualizacje oprogramowania i konfiguracji

Dokumentacja musi opisywać zasady aktualizacji oprogramowania, oprogramowania układowego, konfiguracji i bibliotek zależnych dla zasobów objętych dokumentacją.

Opis musi obejmować co najmniej:

1) komponenty objęte aktualizacją;

2) sposób weryfikacji dostępności aktualizacji;
3) sposób oceny zasadności aktualizacji;
4) sposób oceny wpływu aktualizacji na działanie systemu;
5) wymagane czynności przygotowawcze;
6) wymagane kopie bezpieczeństwa;
7) sposób wykonania aktualizacji;
8) sposób wykonania testów poaktualizacyjnych;
9) sposób wycofania aktualizacji;
10) sposób dokumentowania aktualizacji;
11) ograniczenia dotyczące okien serwisowych;
12) role odpowiedzialne za wykonanie aktualizacji.

Dokumentacja musi jednoznacznie wskazywać, które aktualizacje może wykonywać Zamawiający, a które wymagają udziału Generalnego Wykonawcy, producenta albo autoryzowanego serwisu.

1.2.19.6.14. Zróżnicowanie zawartości ze względu na charakter podsystemów i komponentów

Zakres opisu w „Dokumentacji eksploatacyjnej systemu RIS” musi być dostosowany do charakteru danego zasobu. Generalny Wykonawca zastosuje co najmniej poniższe zróżnicowanie:

1.2.19.6.14.1. Dla oprogramowania aplikacyjnego i usług cyfrowych:

Dokumentacja musi obejmować opis procedur uruchamiania i zatrzymywania usług, monitorowania działania, kontroli logów, zarządzania użytkownikami, wykonywania kopii zapasowych, odtwarzania danych, aktualizacji, obsługi błędów, zależności od baz danych i interfejsów oraz powiązań z innymi usługami systemu RIS.

1.2.19.6.14.2. Dla infrastruktury serwerowej, wirtualizacyjnej i pamięci masowej:

Dokumentacja musi obejmować opis architektury eksploatacyjnej, zasad monitorowania zasobów, procedur startu i zatrzymania, zasad wykonywania kopii zapasowych, zasad odtwarzania, procedur przełączenia awaryjnego, zasad aktualizacji, kontroli pojemności, kontroli obciążenia oraz kontroli stanu sprzętu.

1.2.19.6.14.3. Dla infrastruktury sieciowej, transmisyjnej i cyberbezpieczeństwa:

Dokumentacja musi obejmować opis zasad monitorowania dostępności, kontroli łączności, kontroli parametrów transmisji, kontroli reguł i polityk bezpieczeństwa, procedur odtwarzania konfiguracji, zasad aktualizacji firmware, procedur przełączenia na łącza zapasowe oraz sposobu postępowania przy utracie komunikacji.

1.2.19.6.14.4. Dla urządzeń terenowych, sensorów i komponentów pomiarowych:

Dokumentacja musi obejmować opis sposobu kontroli działania, kontroli transmisji danych, kontroli zasilania, kontroli poprawności pomiarów, kalibracji albo weryfikacji pomiarowej, konserwacji, czyszczenia, diagnostyki lokalnej, wymiany elementów eksploatacyjnych oraz postępowania w przypadku utraty danych albo utraty łączności.

1.2.19.6.14.5. Dla systemów radiokomunikacyjnych i antenowych:

Dokumentacja musi obejmować opis zasad eksploatacji urządzeń radiowych, kontroli kanałów pracy, kontroli dostępności stacji, kontroli torów antenowych, testów łączności, testów redundancji, aktualizacji firmware, diagnostyki kabli, złączy, anten i urządzeń nadawczo-odbiorczych oraz zasad postępowania przy degradacji zasięgu albo jakości sygnału.

1.2.19.6.14.6. Dla systemów CCTV i rejestracji obrazu:

Dokumentacja musi obejmować opis zasad kontroli obrazu, rejestracji, archiwizacji, retencji, odtwarzania nagrań, wykonywania kopii nagrań, kontroli rejestratorów, kontroli dysków, testów przełączenia awaryjnego, utrzymania optyki kamer, korekty ustawień oraz diagnostyki utraty obrazu.

1.2.19.6.14.7. Dla systemów zasilania, klimatyzacji, kontroli dostępu, ochrony przeciwpożarowej i infrastruktury technicznej obiektów:

Dokumentacja musi obejmować opis zasad eksploatacji, kontroli alarmów, testów okresowych, konserwacji, przeglądów wymaganych przez producentów i przepisy prawa, zasad udziału wyspecjalizowanego serwisu oraz wpływu awarii tych systemów na działanie komponentów RIS.

1.2.19.6.14.8. Dla interfejsów integracyjnych i wymiany danych:

Dokumentacja musi obejmować opis punktów integracji, zależności systemowych, formatów wymiany danych, zasad monitorowania interfejsów, typowych błędów, procedur diagnostycznych, zasad restartu usług integracyjnych oraz sposobu potwierdzenia prawidłowej wymiany danych.

1.2.19.6.14.9. Wykazy i zestawienia wymagane w dokumentacji

Generalny Wykonawca zamieści w dokumentacji co najmniej następujące zestawienia:

Tabela 1. Wykaz podsystemów, komponentów i usług objętych dokumentacją

Lp.	Nazwa zasobu	Kategoria	Funkcja w systemie RIS	Lokalizacja	Status: nowy / zmodernizowany / istniejący objęty zakresem	Zakres odpowiedzialności Generalnego Wykonawcy	Dokumenty powiązane	Uwagi

Tabela 2. Wykaz lokalizacji objętych dokumentacją

Lp.	Lokalizacja	Typ obiektu	Zasoby objęte dokumentacją	Zasoby istniejące powiązane	Zasady dostępu	Wymagania BHP / formalne	Uwagi

Tabela 3. Wykaz dokumentów powiązanych

Lp.	Nazwa dokumentu	Wersja	Data	Autor / dostawca	Zakres odwołania	Powiązany zasób	Lokalizacja dokumentu	Uwagi

Tabela 4. Wykaz procedur eksploatacyjnych

Lp.	Nazwa procedury	Podsystem / komponent	Cel procedury	Wymagane uprawnienia	Częstotliwość / tryb wykonania	Wpływ na dostępność systemu	Dokument potwierdzający	Uwagi

Tabela 5. Wykaz testów okresowych i konserwacji

Lp.	Podsystem / komponent	Rodzaj testu lub konserwacji	Częstotliwość	Wykonawca czynności	Warunki wykonania	Oczekiwany wynik	Protokół / raport	Uwagi

Tabela 6. Wykaz procedur awaryjnych

Lp.	Zdarzenie / awaria	Objawy	Wstępna diagnostyka	Czynności Zamawiającego	Czynności serwisowe	Eskalacja	Wymagane dane do zgłoszenia	Uwagi

1.2.19.6.15. Wymagania dotyczące aktualizacji dokumentu

Generalny Wykonawca zaktualizuje „Dokumentację eksploatacyjną systemu RIS” każdorazowo w przypadku:

1) zmiany konfiguracji systemu;
2) zmiany architektury rozwiązania;
3) wymiany, dodania albo usunięcia komponentu;
4) zmiany lokalizacji komponentu;
5) zmiany wersji oprogramowania albo oprogramowania układowego wpływającej na eksploatację;
6) zmiany procedur operacyjnych, testowych, konserwacyjnych albo awaryjnych;
7) zmiany dokumentów powiązanych;
8) zmiany zasad wykonywania kopii zapasowych albo odtwarzania;
9) zmiany wymagań producenta;
10) zmiany zakresu odpowiedzialności Generalnego Wykonawcy;
11) stwierdzenia przez Zamawiającego niekompletności, nieaktualności albo niespójności dokumentu.

Każda aktualizacja dokumentu musi zawierać oznaczenie wersji, datę zmiany, autora zmiany, opis zmiany oraz wskazanie rozdziałów, tabel albo załączników objętych zmianą. Zaktualizowana wersja dokumentu wymaga akceptacji Zamawiającego.

1.2.19.6.16. Wymagania dotyczące formy przekazania

Generalny Wykonawca przekaże dokument w wersji edytowalnej oraz w wersji nieedytowalnej. Wersja edytowalna musi umożliwiać Zamawiającemu późniejszą aktualizację dokumentacji na potrzeby własnej eksploatacji systemu.

Dokument musi być przekazany w strukturze umożliwiającej łatwe wyszukiwanie informacji, weryfikację powiązań z dokumentacją powykonawczą oraz identyfikację procedur właściwych dla danego podsystemu, komponentu, usługi albo lokalizacji.

Załączniki, instrukcje, pliki konfiguracyjne, listy kontrolne, wzory protokołów oraz inne materiały powiązane muszą zostać przekazane w uporządkowanym repozytorium dokumentacji wraz z indeksem zawartości.

1.2.19.6.17. Warunki akceptacji dokumentu

Zamawiający zaakceptuje „Dokumentację eksploatacyjną systemu RIS” po potwierdzeniu, że dokument:

1) obejmuje pełny zakres zasobów objętych odpowiedzialnością Generalnego Wykonawcy;
2) jednoznacznie wskazuje zasoby objęte dokumentacją oraz zasoby istniejące wyłączone z dokumentacji;
3) jest zgodny z dokumentacją projektową, powykonawczą, instalacyjną i konfiguracyjną;
4) zawiera wykaz dokumentów powiązanych;
5) zawiera procedury operacyjne dla zasobów objętych dokumentacją;
6) zawiera opis metod zapewnienia wymaganego poziomu niezawodności;
7) zawiera procedury testów okresowych i konserwacji;
8) zawiera procedury awaryjne i diagnostyczne;
9) zawiera zasady wykonywania kopii zapasowych i odtwarzania, jeżeli dotyczy;
10) zawiera zasady aktualizacji oprogramowania, firmware i konfiguracji, jeżeli dotyczy;
11) wskazuje czynności możliwe do wykonania przez Zamawiającego oraz czynności wymagające udziału Generalnego Wykonawcy, producenta, autoryzowanego serwisu albo osoby posiadającej wymagane uprawnienia;
12) zawiera wymagane tabele, wykazy, formularze, listy kontrolne i załączniki;
13) jest spójny terminologicznie i redakcyjnie;
14) umożliwia praktyczne wykorzystanie dokumentu w bieżącej eksploatacji systemu RIS.

1.2.20. Procedury odbioru i testowania całości systemu RIS

Niniejszy rozdział określa ogólne wymagania Zamawiającego dotyczące organizacji, przygotowania, przeprowadzenia, udokumentowania i zatwierdzenia odbiorów oraz testów całości systemu RIS realizowanego w ramach przedmiotu zamówienia.

1) Procedury odbioru i testowania całości systemu RIS muszą obejmować wszystkie elementy dostarczone, wykonane, zainstalowane, skonfigurowane, zmodernizowane, rozbudowane, wymienione, zintegrowane albo objęte odpowiedzialnością Generalnego Wykonawcy w ramach realizacji przedmiotu zamówienia.
2) Procedury odbioru i testowania całości systemu RIS nie zastępują szczegółowych wymagań odbiorowych, testowych i pomiarowych określonych w pozostałych rozdziałach PFU oraz w dokumentach branżowych, w szczególności w Planie systemu monitoringu wizyjnego CCTV, Planie łączności radiowej VHF/AIS oraz Planie połączeń transmisyjnych. Wymagania określone w niniejszym rozdziale należy stosować łącznie z wymaganiami szczegółowymi właściwymi dla poszczególnych podsystemów, urządzeń, lokalizacji, usług, interfejsów, integracji, dokumentacji i robót.
3) Celem odbioru i testowania całości systemu RIS jest potwierdzenie, że przedmiot zamówienia został wykonany kompletnie, zgodnie z PFU, dokumentacją projektową, dokumentacją branżową, ofertą Generalnego Wykonawcy, wymaganiami producentów, warunkami uzgodnień, obowiązującymi przepisami prawa, normami, standardami oraz zasadami wiedzy technicznej, a także że może zostać przekazany Zamawiającemu do bezpiecznej, stabilnej i zgodnej z przeznaczeniem eksploatacji.

4) Generalny Wykonawca zobowiązany jest opracować i uzgodnić z Zamawiającym Plan Odbiorów i Testów Systemu RIS. Dokument ten musi zostać przekazany Zamawiającemu do akceptacji przed rozpoczęciem zasadniczych testów odbiorowych oraz przed przystąpieniem do odbiorów częściowych, branżowych, integracyjnych lub końcowych.
5) Plan Odbiorów i Testów Systemu RIS musi określać co najmniej:
   a) zakres testów i odbiorów dla poszczególnych podsystemów, komponentów, lokalizacji, usług cyfrowych, integracji i elementów infrastruktury;
   b) podział testów na testy częściowe, branżowe, lokalizacyjne, funkcjonalne, niefunkcjonalne, integracyjne, bezpieczeństwa, wydajnościowe, niezawodnościowe, transmisyjne, eksploatacyjne i końcowe;
   c) powiązanie testów z wymaganiami PFU, dokumentami branżowymi, dokumentacją projektową, dokumentacją powykonawczą i dokumentacją producentów;
   d) opis środowisk, lokalizacji, urządzeń, danych, kont użytkowników i konfiguracji wykorzystywanych w testach;
   e) role i odpowiedzialności Generalnego Wykonawcy, Zamawiającego, producentów, podwykonawców i innych podmiotów uczestniczących w testach;
   f) harmonogram testów i odbiorów;
   g) warunki rozpoczęcia poszczególnych kategorii testów;
   h) scenariusze testowe albo odwołanie do scenariuszy testowych określonych w dokumentach szczegółowych;
   i) kryteria zaliczenia i niezaliczenia testów;
   j) zasady dokumentowania przebiegu testów;
   k) zasady rejestrowania, klasyfikacji, obsługi i zamykania błędów, usterek, wad, niezgodności i obserwacji;
   l) zasady powtarzania testów po usunięciu wad lub zmianie konfiguracji;
   m) wzory protokołów testowych, raportów z testów, list kontrolnych i protokołów odbioru;
   n) wymagania dotyczące kompletności dokumentacji, licencji, konfiguracji, dostępów, kopii zapasowych i materiałów przekazywanych Zamawiającemu;
   o) warunki dopuszczenia przedmiotu zamówienia do Odbioru Końcowego.
6) Testy i odbiory muszą być prowadzone w sposób umożliwiający jednoznaczne potwierdzenie zgodności wykonania co najmniej w następujących obszarach:
   a) kompletność rzeczowa dostaw, robót, instalacji, konfiguracji, licencji, usług, dokumentacji i integracji;
   b) zgodność z dokumentacją projektową i powykonawczą;
   c) poprawność działania urządzeń terenowych, sensorów, kamer, stacji radiowych, urządzeń transmisyjnych, zasilania, szaf teletechnicznych, konstrukcji wsporczych i infrastruktury serwerowej;
   d) poprawność działania usług cyfrowych, aplikacji, API, mechanizmów integracyjnych i wymiany danych;

e) poprawność komunikacji pomiędzy lokalizacjami terenowymi, Centrum RIS, środowiskiem pracy zmodernizowanego systemu RIS, serwerownią zapasową oraz systemami zewnętrznymi;

f) osiągnięcie wymaganych parametrów transmisyjnych, przepustowości, opóźnień, niezawodności, redundancji, przełączenia awaryjnego i separacji ruchu;

g) osiągnięcie wymaganych parametrów funkcjonalnych i użytkowych systemu CCTV;

h) osiągnięcie wymaganych parametrów funkcjonalnych i użytkowych systemu VHF/AIS/DGNSS;

i) osiągnięcie wymaganych parametrów czujników hydrologicznych i meteorologicznych oraz poprawności przetwarzania, buforowania i przekazywania danych pomiarowych;

j) poprawność działania mechanizmów wysokiej dostępności, replikacji, backupu, odtwarzania, monitoringu technicznego, alarmowania i logowania;

k) poprawność działania mechanizmów cyberbezpieczeństwa, kontroli dostępu, autoryzacji, uwierzytelniania, segmentacji, szyfrowania i audytowalności;

l) poprawność działania procedur operacyjnych, awaryjnych, utrzymaniowych i administracyjnych;

m) kompletność i zgodność dokumentacji przekazywanej Zamawiającemu;

n) gotowość systemu do przekazania do eksploatacji.

7) W ramach odbiorów i testów Generalny Wykonawca zobowiązany jest przeprowadzić co najmniej:

a) odbiory dokumentacji projektowej, wykonawczej, konfiguracyjnej, testowej, odbiorowej, powykonawczej, eksploatacyjnej, administratora i użytkownika;

b) odbiory dostaw sprzętu, licencji, oprogramowania, urządzeń, materiałów i wyposażenia;

c) odbiory robót budowlanych, instalacyjnych, montażowych, teletechnicznych, energetycznych, kablowych i konfiguracyjnych;

d) odbiory lokalizacyjne dla poszczególnych obiektów terenowych;

e) odbiory branżowe dla poszczególnych podsystemów;

f) testy funkcjonalne i niefunkcjonalne;

g) testy integracyjne pomiędzy podsystemami RIS;

h) testy integracji z systemami zewnętrznymi;

i) testy transmisji danych i redundancji torów dostępowych;

j) testy bezpieczeństwa, dostępności, logowania i monitorowania;

k) testy odtworzeniowe, awaryjne i ciągłości działania;

l) testy gotowości operacyjnej;

m) testy regresji po usunięciu wad albo zmianach konfiguracji;

n) testy końcowe całości systemu RIS.

8) Odbiory częściowe, branżowe i lokalizacyjne mogą zostać dokonane wyłącznie w zakresie elementów kompletnych, uruchomionych, skonfigurowanych, udokumentowanych i przetestowanych w stopniu umożliwiającym ich obiektywną ocenę przez Zamawiającego.
9) Odbiór Końcowy całości systemu RIS może nastąpić wyłącznie po spełnieniu łącznie następujących warunków:
   a) wykonaniu całości przedmiotu zamówienia;
   b) zakończeniu wszystkich wymaganych odbiorów częściowych, branżowych, lokalizacyjnych i integracyjnych;
   c) pozytywnym zakończeniu testów końcowych całości systemu RIS;
   d) usunięciu wszystkich wad, usterek i niezgodności blokujących odbiór albo istotnie ograniczających funkcjonalność, bezpieczeństwo, niezawodność lub możliwość eksploatacji systemu;
   e) przekazaniu i zaakceptowaniu przez Zamawiającego wymaganej dokumentacji;
   f) przekazaniu kompletnej dokumentacji powykonawczej, konfiguracyjnej, eksploatacyjnej, administratora i użytkownika;
   g) przekazaniu licencji, kluczy, certyfikatów, kont administracyjnych, haseł, konfiguracji, kopii konfiguracji, instrukcji odtworzeniowych i danych niezbędnych do administrowania systemem;
   h) przeprowadzeniu wymaganych szkoleń;
   i) potwierdzeniu gotowości Zamawiającego do przejęcia systemu do eksploatacji;
   j) podpisaniu protokołów odbioru wymaganych dla danego etapu.
10) Generalny Wykonawca nie może uzależniać pozytywnego wyniku odbioru od zastosowania procedur, narzędzi, kont, licencji, konfiguracji albo uprawnień niedostępnych Zamawiającemu po zakończeniu realizacji przedmiotu zamówienia.
11) Wszystkie czynności testowe i odbiorowe muszą być dokumentowane w formie protokołów, raportów, zrzutów konfiguracji, wyników pomiarów, logów, list kontrolnych, zdjęć, zestawień, wydruków albo innych dowodów potwierdzających wykonanie i wynik testu. Dokumentacja ta stanowi część dokumentacji odbiorowej i powykonawczej.
12) W przypadku stwierdzenia wad, usterek, błędów, braków, niezgodności albo odchyleń od wymagań PFU Generalny Wykonawca zobowiązany jest do ich usunięcia na własny koszt, aktualizacji dokumentacji oraz ponownego przeprowadzenia testów w zakresie wymaganym przez Zamawiającego.
13) Pozytywny wynik testów i odbiorów częściowych nie zwalnia Generalnego Wykonawcy z odpowiedzialności za poprawne działanie całości systemu RIS oraz za usunięcie wad ujawnionych w toku testów integracyjnych, końcowych, eksploatacyjnych, gwarancyjnych albo w okresie świadczenia usług serwisowych.
14) Zamawiający ma prawo odmówić dokonania odbioru, jeżeli przedmiot odbioru nie jest kompletny, nie został przetestowany, nie posiada wymaganej dokumentacji, nie spełnia wymagań funkcjonalnych, niefunkcjonalnych, bezpieczeństwa, dostępności,

niezawodności, transmisji, integracji albo nie może zostać bezpiecznie przekazany do eksploatacji.

1.2.21. Szkolenia, procedury operacyjne i przekazanie do eksploatacji

Niniejszy rozdział określa wymagania Zamawiającego dotyczące przygotowania i przeprowadzenia szkoleń, opracowania oraz przekazania procedur operacyjnych, a także formalnego i technicznego przekazania systemu RIS do eksploatacji.

1) Generalny Wykonawca zobowiązany jest zapewnić przygotowanie Zamawiającego do samodzielnej, bezpiecznej i prawidłowej eksploatacji, administrowania, monitorowania, utrzymania i nadzorowania wszystkich elementów systemu RIS objętych przedmiotem zamówienia.
2) Generalny Wykonawca opracuje i przekaże Zamawiającemu Plan Szkoleń oraz Przekazania do Eksploatacji. Dokument ten musi zostać uzgodniony z Zamawiającym przed rozpoczęciem szkoleń i czynności przekazania systemu do eksploatacji.
3) Plan Szkoleń oraz Przekazania do Eksploatacji musi określać co najmniej:
   a) grupy uczestników szkoleń;
   b) zakres tematyczny szkoleń dla poszczególnych grup;
   c) formę prowadzenia szkoleń;
   d) czas trwania szkoleń;
   e) wymagania dotyczące materiałów szkoleniowych;
   f) wymagania dotyczące środowiska szkoleniowego;
   g) harmonogram szkoleń;
   h) sposób potwierdzenia udziału uczestników;
   i) sposób weryfikacji nabycia wiedzy i umiejętności;
   j) zakres wsparcia udzielanego Zamawiającemu w okresie przekazania do eksploatacji;
   k) listę procedur operacyjnych przekazywanych Zamawiającemu;
   l) warunki formalnego potwierdzenia gotowości systemu do eksploatacji.
4) Szkolenia muszą obejmować co najmniej następujące grupy użytkowników i personelu Zamawiającego:
   a) operatorów Centrum RIS;
   b) administratorów systemu RIS;
   c) administratorów infrastruktury serwerowej, wirtualizacyjnej, pamięci masowej, backupu i środowiska pracy systemu RIS;
   d) administratorów sieci, transmisji danych, urządzeń bezpieczeństwa i połączeń VPN;
   e) osoby odpowiedzialne za obsługę systemu CCTV;
   f) osoby odpowiedzialne za obsługę systemu VHF/AIS/DGNSS;

g) osoby odpowiedzialne za obsługę danych hydrologicznych, meteorologicznych i usług cyfrowych;

h) osoby odpowiedzialne za monitoring techniczny, diagnostykę i obsługę alarmów;

i) osoby odpowiedzialne za cyberbezpieczeństwo, kontrolę dostępu, logowanie, incydenty i podatności;

j) osoby odpowiedzialne za utrzymanie, serwis, przeglądy i współpracę z Generalnym Wykonawcą w okresie gwarancji.

5) Szkolenia muszą być prowadzone w języku polskim. Materiały szkoleniowe, instrukcje, prezentacje, ćwiczenia, scenariusze, listy kontrolne i dokumenty potwierdzające udział w szkoleniach muszą zostać opracowane i przekazane Zamawiającemu w języku polskim.

6) Zakres szkoleń musi być dostosowany do charakteru danej grupy uczestników i obejmować odpowiednio:

a) architekturę systemu RIS po rozbudowie i modernizacji;

b) zakres funkcjonalny poszczególnych podsystemów;

c) obsługę operatorską usług RIS;

d) obsługę systemu CCTV, w tym podgląd, odtwarzanie, eksport, maski prywatności, uprawnienia, alarmy i scenariusze awaryjne;

e) obsługę systemu VHF/AIS/DGNSS, w tym funkcje operatorskie, monitorowanie stacji, alarmy, diagnostykę i podstawowe procedury awaryjne;

f) obsługę danych hydrologicznych i meteorologicznych, w tym kontrolę jakości danych, korekty, transmisję, buforowanie i udostępnianie danych;

g) obsługę usług cyfrowych RIS oraz interfejsów API;

h) administrowanie użytkownikami, rolami, uprawnieniami i dostępami;

i) monitorowanie działania systemu, obsługę alarmów, zdarzeń i logów;

j) wykonywanie kopii zapasowych, odtwarzanie konfiguracji i procedury awaryjne;

k) obsługę mechanizmów wysokiej dostępności, replikacji i przełączenia awaryjnego;

l) zasady bezpiecznej eksploatacji, cyberbezpieczeństwa i reagowania na incydenty;

m) zasady zgłaszania awarii, usterek, problemów, podatności i żądań serwisowych;

n) zasady korzystania z dokumentacji administratora, użytkownika, eksploatacyjnej i powykonawczej.

7) Szkolenia muszą obejmować część teoretyczną oraz część praktyczną. Część praktyczna musi być realizowana z wykorzystaniem środowiska, urządzeń, konfiguracji, ekranów, danych, procedur i scenariuszy odpowiadających rzeczywistemu środowisku eksploatacyjnemu systemu RIS.

8) Generalny Wykonawca zobowiązany jest sporządzić dokumentację przeprowadzonych szkoleń obejmującą co najmniej:

a) program szkolenia;

b) listę uczestników;

c) termin i miejsce szkolenia;

d) imię i nazwisko prowadzącego;

e) materiały szkoleniowe;

f) zakres ćwiczeń praktycznych;

g) wyniki weryfikacji wiedzy, jeżeli została przeprowadzona;

h) zgłoszone pytania, uwagi i rekomendacje;

i) protokół przeprowadzenia szkolenia.

9) Generalny Wykonawca zobowiązany jest opracować i przekazać Zamawiającemu komplet procedur operacyjnych niezbędnych do eksploatacji systemu RIS. Procedury operacyjne mogą stanowić część Dokumentacji eksploatacyjnej systemu RIS, Dokumentacji Administratora, Dokumentacji Użytkownika albo odrębny dokument, pod warunkiem zachowania spójności, kompletności i jednoznacznych odwołań pomiędzy dokumentami.

10) Procedury operacyjne muszą obejmować co najmniej:

a) uruchamianie i zatrzymywanie usług oraz komponentów systemu;

b) bieżące monitorowanie pracy systemu;

c) obsługę alarmów i zdarzeń;

d) diagnostykę podstawowych problemów;

e) obsługę awarii lokalizacji terenowej, utraty łączności, utraty zasilania, utraty urządzenia, utraty usługi albo degradacji parametrów;

f) obsługę mechanizmów wysokiej dostępności i przełączania awaryjnego;

g) wykonywanie i weryfikację kopii zapasowych;

h) odtwarzanie konfiguracji, usług i danych;

i) kontrolę poprawności transmisji danych;

j) kontrolę poprawności danych hydrologicznych i meteorologicznych;

k) obsługę systemu CCTV, w tym retencję, odtwarzanie i eksport materiału;

l) obsługę systemu VHF/AIS/DGNSS;

m) obsługę API i integracji z systemami zewnętrznymi;

n) zarządzanie użytkownikami, rolami i uprawnieniami;

o) zarządzanie zmianą konfiguracyjną;

p) aktualizacje oprogramowania i konfiguracji;

q) obsługę podatności, incydentów bezpieczeństwa i zdarzeń cyberbezpieczeństwa;

r) zgłaszanie i obsługę zgłoszeń serwisowych;

s) przekazywanie informacji do Generalnego Wykonawcy, producentów, podwykonawców albo innych podmiotów wsparcia;

t) dokumentowanie czynności eksploatacyjnych.

11) Przekazanie systemu RIS do eksploatacji musi zostać poprzedzone potwierdzeniem przez Generalnego Wykonawcę, że:
    a) system został wykonany i uruchomiony zgodnie z PFU;
    b) zakończono wymagane testy i odbiory;
    c) usunięto wady i niezgodności uniemożliwiające eksploatację;
    d) przekazano kompletną dokumentację;
    e) przeprowadzono wymagane szkolenia;
    f) przekazano wszystkie konta, role, uprawnienia, hasła, klucze, certyfikaty, licencje, konfiguracje, kody, skrypty, repozytoria, instrukcje i dane niezbędne do eksploatacji;
    g) uruchomiono monitoring techniczny, logowanie i alarmowanie;
    h) skonfigurowano backup, replikację i odtwarzanie;
    i) potwierdzono funkcjonowanie kanałów zgłoszeń serwisowych;
    j) wskazano osoby kontaktowe Generalnego Wykonawcy i producentów;
    k) przekazano wykaz gwarancji, licencji, subskrypcji, terminów wsparcia i warunków serwisowych;
    l) przekazano procedury działania w okresie gwarancji i obsługi technicznej.
12) Generalny Wykonawca zobowiązany jest zapewnić wsparcie Zamawiającego w początkowym okresie eksploatacji systemu RIS, obejmujące co najmniej bieżące konsultacje, wsparcie operatorów i administratorów, analizę zgłoszeń, wyjaśnianie działania systemu, wsparcie w obsłudze incydentów, korektę dokumentacji oraz usuwanie usterek ujawnionych po przekazaniu systemu do eksploatacji.
13) Przekazanie do eksploatacji musi zostać potwierdzone protokołem podpisanym przez Strony. Protokół musi zawierać co najmniej:
    a) datę przekazania do eksploatacji;
    b) zakres przekazywanych elementów;
    c) wykaz dokumentacji;
    d) wykaz kont, dostępów, licencji i konfiguracji;
    e) wykaz przeprowadzonych szkoleń;
    f) wykaz otwartych uwag, jeżeli Zamawiający dopuści przekazanie systemu z uwagami niemającymi wpływu na bezpieczeństwo, ciągłość działania i możliwość eksploatacji;
    g) wskazanie daty rozpoczęcia okresu gwarancji, serwisu i obsługi technicznej, jeżeli zgodnie z umową jest ona powiązana z przekazaniem systemu albo Odbiorem Końcowym.
14) Przekazanie systemu RIS do eksploatacji nie zwalnia Generalnego Wykonawcy z odpowiedzialności za usunięcie wad, usterek, błędów, braków dokumentacyjnych, problemów konfiguracyjnych i niezgodności ujawnionych po przekazaniu systemu, w szczególności w okresie gwarancji, serwisu, obsługi technicznej i SLA.

1.2.22. Gwarancja, serwis, obsługa techniczna i SLA

Niniejszy rozdział określa ogólne wymagania Zamawiającego dotyczące gwarancji, serwisu, obsługi technicznej oraz zasad świadczenia usług SLA dla przedmiotu zamówienia.

1) Wymagania określone w niniejszym rozdziale należy stosować łącznie z wymaganiami dotyczącymi przeglądów technicznych i aktualizacji oprogramowania w okresie gwarancji, Usługi Utrzymania, dokumentacji eksploatacyjnej, cyberbezpieczeństwa, monitoringu technicznego, procedur odbioru i testowania, procedur operacyjnych oraz wymaganiami szczegółowymi określonymi dla poszczególnych podsystemów, urządzeń, instalacji, usług, integracji i dokumentów.
2) Okres gwarancji na całość przedmiotu zamówienia wynosi X, liczony od dnia podpisania przez Strony Protokołu Odbioru Końcowego bez zastrzeżeń, chyba że Umowa stanowi inaczej albo dokumenty gwarancyjne producenta przewidują dłuższy okres gwarancji lub wsparcia dla danego komponentu. W takim przypadku zastosowanie ma okres korzystniejszy dla Zamawiającego.
3) Szczegółowe parametry gwarancji, serwisu, obsługi technicznej i SLA, w tym w szczególności czasy potwierdzenia przyjęcia zgłoszenia, czasy reakcji, czasy rozpoczęcia pracy zdalnej, czasy przyjazdu serwisu na miejsce, czasy przedstawienia diagnozy, czasy przedstawienia obejścia, czasy usunięcia awarii lub usterki, godziny świadczenia wsparcia, tryb obsługi zgłoszeń, zasady eskalacji, zasady raportowania, katalog usług krytycznych, katalog komponentów krytycznych, zasady naliczania dostępności, zasady obsługi prac planowych, zasady usuwania podatności, zasady naliczania kar umownych oraz pozostałe parametry świadczenia usług gwarancyjnych i serwisowych zostaną określone w Umowie lub załącznikach do Umowy.
4) Generalny Wykonawca zobowiązany jest świadczyć gwarancję, serwis, obsługę techniczną i SLA zgodnie z wymaganiami PFU, Umową, dokumentacją producentów, dokumentacją eksploatacyjną, Szczegółowym Planem Przeglądów i Aktualizacji, Dokumentacją eksploatacyjną systemu RIS oraz innymi dokumentami zatwierdzonymi przez Zamawiającego.
5) W przypadku rozbieżności pomiędzy wymaganiami PFU a postanowieniami Umowy dotyczącymi szczegółowych parametrów gwarancji, serwisu, obsługi technicznej i SLA, zastosowanie mają postanowienia Umowy, o ile nie obniżają one minimalnego zakresu odpowiedzialności Generalnego Wykonawcy wynikającego z PFU, dokumentacji projektowej, dokumentacji branżowej, przepisów prawa, norm, gwarancji producentów oraz zaakceptowanej dokumentacji powykonawczej i eksploatacyjnej.
6) Gwarancja musi obejmować wszystkie elementy dostarczone, wykonane, zainstalowane, skonfigurowane, zmodernizowane, rozbudowane, wymienione, zintegrowane albo objęte odpowiedzialnością Generalnego Wykonawcy w ramach przedmiotu zamówienia, w szczególności:
    a) roboty budowlane, instalacyjne, montażowe, teletechniczne, energetyczne i kablowe;
    b) wieże, maszty, słupy, konstrukcje wsporcze, fundamenty, ogrodzenia, platformy, systemy asekuracyjne, instalacje odgromowe, uziemienia i zabezpieczenia przepięciowe;

c) szafy teletechniczne typu zewnętrznego oraz ich wyposażenie;

d) urządzenia VHF/AIS/DGNSS, systemy antenowe, tory antenowe i urządzenia współpracujące;

e) kamery, rejestratory, platformę rejestracji, stacje klienckie, urządzenia prezentacji obrazu i elementy systemu CCTV;

f) czujniki hydrologiczne, sensory meteorologiczne, lokalne komponenty akwizycji danych, urządzenia przetwarzania danych i układy transmisji danych pomiarowych;

g) urządzenia sieciowe, transmisyjne, bezpieczeństwa, VPN, routery, przełączniki, modemy, urządzenia radiowe i światłowodowe;

h) infrastrukturę serwerową, macierze, urządzenia backupu, oprogramowanie systemowe, wirtualizacyjne, bazodanowe, monitorujące, backupowe i zarządzające;

i) środowisko pracy zmodernizowanego systemu RIS;

j) elementy serwerowni głównej, serwerowni zapasowej, łącza teleinformatycznego i infrastruktury Data Center objętej odpowiedzialnością Generalnego Wykonawcy;

k) usługi cyfrowe RIS, API, integracje, konfiguracje, skrypty, interfejsy, mechanizmy wymiany danych i dokumentację techniczną;

l) dokumentację projektową, powykonawczą, administratora, użytkownika, eksploatacyjną, testową, odbiorową, gwarancyjną i serwisową.

7) Generalny Wykonawca odpowiada za zapewnienie, aby wszystkie dostarczone komponenty były objęte gwarancją i wsparciem producenta przez okres wymagany w PFU i Umowie. Brak gwarancji producenta, brak aktywnego wsparcia, brak licencji, brak subskrypcji albo brak uprawnienia serwisowego nie może ograniczać możliwości korzystania przez Zamawiającego z systemu RIS ani skutecznego dochodzenia uprawnień gwarancyjnych.

8) W okresie gwarancji Generalny Wykonawca zobowiązany jest na własny koszt usuwać wszystkie wady, usterki, awarie, błędy, niezgodności, problemy konfiguracyjne, problemy integracyjne, problemy wydajnościowe, problemy bezpieczeństwa i inne nieprawidłowości ujawnione w przedmiocie zamówienia, niezależnie od tego, czy ich przyczyna dotyczy sprzętu, oprogramowania, konfiguracji, instalacji, dokumentacji, integracji, transmisji, robót, montażu, danych, procedur albo współdziałania komponentów.

9) Usunięcie wady albo awarii musi obejmować wszystkie czynności niezbędne do przywrócenia prawidłowego działania systemu, w szczególności diagnostykę, dostawę części, wymianę urządzeń, naprawę, rekonfigurację, aktualizację, odtworzenie konfiguracji, odtworzenie danych, testy po naprawie, aktualizację dokumentacji oraz przekazanie Zamawiającemu raportu z wykonanych czynności.

10) Generalny Wykonawca zobowiązany jest zapewnić serwis i obsługę techniczną w sposób umożliwiający utrzymanie ciągłości działania systemu RIS, bezpieczeństwa przetwarzanych danych, dostępności usług, poprawności transmisji danych, gotowości lokalizacji terenowych, poprawności działania usług cyfrowych, integracji i monitoringu technicznego.

11) Generalny Wykonawca zobowiązany jest zapewnić jeden punkt kontaktu dla zgłoszeń gwarancyjnych, serwisowych i technicznych. Punkt kontaktu musi umożliwiać co najmniej:

a) przyjmowanie zgłoszeń awarii, usterek, błędów, problemów, niezgodności i pytań technicznych;

b) nadawanie numerów zgłoszeń;

c) potwierdzanie przyjęcia zgłoszeń;

d) klasyfikację zgłoszeń;

e) śledzenie statusu zgłoszeń;

f) komunikację z Zamawiającym;

g) eskalację zgłoszeń;

h) raportowanie obsługi zgłoszeń;

i) dokumentowanie czasu potwierdzenia przyjęcia zgłoszenia, czasu reakcji, czasu przedstawienia diagnozy, czasu przedstawienia obejścia, czasu naprawy i czasu zamknięcia zgłoszenia.

12) Zgłoszenia serwisowe muszą być klasyfikowane co najmniej według następujących kategorii:

a) awaria krytyczna – zdarzenie powodujące niedostępność całości systemu RIS, istotnej usługi RIS, krytycznej funkcji Centrum RIS, środowiska pracy systemu RIS, istotnego elementu infrastruktury centralnej, krytycznej integracji, istotnej funkcji bezpieczeństwa albo zdarzenie mogące powodować utratę danych, naruszenie bezpieczeństwa lub istotne zagrożenie ciągłości działania;

b) awaria istotna – zdarzenie powodujące niedostępność lub poważną degradację działania jednego podsystemu, lokalizacji, usługi, funkcji, integracji, komponentu albo grupy użytkowników, przy zachowaniu możliwości ograniczonej pracy systemu;

c) usterka zwykła – zdarzenie powodujące ograniczenie funkcjonalności, błąd, niezgodność, problem eksploatacyjny albo degradację parametrów, które nie powoduje istotnego zagrożenia dla ciągłości działania systemu;

d) zgłoszenie konsultacyjne lub administracyjne – pytanie techniczne, prośba o wyjaśnienie, wsparcie administracyjne, weryfikacja konfiguracji albo inne zgłoszenie niewynikające z awarii lub usterki.

13) Dla każdej kategorii zgłoszeń Generalny Wykonawca zobowiązany jest dotrzymywać parametrów gwarancji, serwisu, obsługi technicznej i SLA określonych w Umowie. Parametry te będą obejmować w szczególności czas potwierdzenia przyjęcia zgłoszenia, czas reakcji serwisowej, czas rozpoczęcia pracy zdalnej, czas przyjazdu serwisu na miejsce, czas przedstawienia diagnozy, czas przedstawienia obejścia, czas usunięcia awarii lub usterki, zasady eskalacji, zasady raportowania oraz zasady naliczania przekroczeń SLA.

14) W przypadku awarii krytycznych Generalny Wykonawca musi zapewnić obsługę zgłoszeń w trybie zapewniającym ciągłość działania systemu RIS, z uwzględnieniem możliwości pracy poza standardowymi godzinami pracy Zamawiającego, jeżeli charakter awarii, jej wpływ na bezpieczeństwo, dostępność usług, integralność danych albo ciągłość działania tego wymaga, zgodnie z zasadami określonymi w Umowie.

15) W przypadku awarii dotyczących cyberbezpieczeństwa, podatności, naruszenia poufności, integralności, dostępności lub autentyczności danych, Generalny Wykonawca zobowiązany jest działać zgodnie z wymaganiami dotyczącymi cyberbezpieczeństwa, Polityki Zarządzania Podatnościami, Usługi Utrzymania oraz procedurami uzgodnionymi z Zamawiającym i określonymi w dokumentacji projektowej, eksploatacyjnej lub Umowie.

16) W okresie gwarancji Generalny Wykonawca zobowiązany jest utrzymywać zdolność serwisową obejmującą co najmniej:

   a) dostęp do personelu posiadającego kompetencje techniczne właściwe dla dostarczonych rozwiązań;

   b) dostęp do wsparcia producentów;

   c) dostęp do części zamiennych, urządzeń zastępczych, licencji, aktualizacji i narzędzi diagnostycznych;

   d) możliwość realizacji prac zdalnych i lokalnych;

   e) możliwość wykonywania czynności serwisowych w lokalizacjach terenowych, Centrum RIS, serwerowni głównej, serwerowni zapasowej oraz innych lokalizacjach objętych przedmiotem zamówienia;

   f) możliwość wykonywania testów po naprawie;

   g) możliwość aktualizacji dokumentacji po wykonanych czynnościach.

17) Generalny Wykonawca zobowiązany jest zapewnić, aby wymiana urządzenia, komponentu, części, modułu, licencji albo oprogramowania w okresie gwarancji nie powodowała obniżenia parametrów funkcjonalnych, technicznych, wydajnościowych, bezpieczeństwa, trwałości, niezawodności, interoperacyjności ani warunków eksploatacji systemu RIS.

18) Wymieniane urządzenia, komponenty i części muszą być fabrycznie nowe, pełnowartościowe, zgodne albo równoważne funkcjonalnie i technicznie z elementami wymienianymi, pochodzić z autoryzowanego kanału sprzedaży producenta albo autoryzowanego partnera oraz być objęte gwarancją i wsparciem producenta przez okres nie krótszy niż pozostały okres gwarancji dla przedmiotu zamówienia.

19) W przypadku uszkodzenia nośnika danych, nośnik po wymianie pozostaje u Zamawiającego, jeżeli był wykorzystywany do przechowywania danych, konfiguracji, logów, nagrań, kopii zapasowych, danych pomiarowych albo innych informacji systemu RIS, chyba że Umowa stanowi inaczej w sposób korzystniejszy dla Zamawiającego.

20) Generalny Wykonawca zobowiązany jest prowadzić rejestr zgłoszeń gwarancyjnych, serwisowych i technicznych. Rejestr musi umożliwiać weryfikację co najmniej:

   a) numeru zgłoszenia;

   b) daty i godziny zgłoszenia;

   c) osoby lub jednostki zgłaszającej;

   d) opisu zgłoszenia;

   e) kategorii zgłoszenia;

   f) wpływu zgłoszenia na działanie systemu;

g) podjętych czynności;

h) czasu potwierdzenia, reakcji, diagnozy, obejścia, naprawy i zamknięcia;

i) podmiotów uczestniczących w obsłudze zgłoszenia;

j) zastosowanych części, aktualizacji, zmian konfiguracyjnych i poprawek;

k) wyniku testów po naprawie;

l) statusu zgłoszenia;

m) przekroczeń SLA i działań korygujących.

21) Generalny Wykonawca zobowiązany jest przekazywać Zamawiającemu raporty z obsługi gwarancyjnej, serwisowej i technicznej zgodnie z zasadami określonymi w Umowie. Raporty muszą obejmować co najmniej:

a) wykaz zgłoszeń w okresie raportowym;

b) status zgłoszeń otwartych i zamkniętych;

c) klasyfikację zgłoszeń;

d) czasy obsługi zgłoszeń;

e) przekroczenia SLA;

f) działania korygujące i zapobiegawcze;

g) wykaz wymienionych urządzeń, części, modułów i licencji;

h) wykaz aktualizacji oprogramowania i konfiguracji;

i) wykaz powtarzających się problemów;

j) rekomendacje zmian eksploatacyjnych, konfiguracyjnych lub organizacyjnych;

k) wpływ zgłoszeń na dostępność systemu RIS.

22) Generalny Wykonawca zobowiązany jest wykonywać czynności serwisowe i gwarancyjne w sposób minimalizujący wpływ na działanie systemu RIS. Czynności planowe, aktualizacje, rekonfiguracje, prace wymagające przerwy w działaniu albo obniżenia dostępności usług muszą być uzgadniane z Zamawiającym i wykonywane w uzgodnionych oknach serwisowych, zgodnie z zasadami określonymi w Umowie.

23) Generalny Wykonawca zobowiązany jest każdorazowo poinformować Zamawiającego o ryzyku związanym z planowaną czynnością serwisową, w szczególności o ryzyku przerwy w działaniu, utraty danych, degradacji parametrów, wpływie na integracje, wpływie na bezpieczeństwo oraz sposobie przywrócenia stanu poprzedniego.

24) Po wykonaniu czynności serwisowych, naprawczych, gwarancyjnych, aktualizacyjnych albo konfiguracyjnych Generalny Wykonawca zobowiązany jest wykonać testy potwierdzające prawidłowe działanie objętych nimi komponentów oraz przekazać Zamawiającemu informację o wyniku testów.

25) W okresie gwarancji Generalny Wykonawca zobowiązany jest aktualizować dokumentację powykonawczą, konfiguracyjną, eksploatacyjną, administratora, użytkownika, gwarancyjną i serwisową w zakresie wynikającym z wykonanych napraw, wymian, aktualizacji, zmian konfiguracji, zmian licencyjnych, zmian topologii, zmian procedur albo innych czynności mających wpływ na stan systemu RIS.

26) Generalny Wykonawca zobowiązany jest wykonywać w okresie gwarancji przeglądy techniczne, konserwacje, aktualizacje, kontrole i czynności utrzymaniowe wymagane dla dostarczonych, wykonanych, zmodernizowanych, rozbudowanych, wymienionych, skonfigurowanych albo objętych jego odpowiedzialnością elementów systemu RIS. Zakres, częstotliwość i sposób wykonywania tych czynności muszą być zgodne z PFU, dokumentacją producentów, Szczegółowym Planem Przeglądów i Aktualizacji, Dokumentacją eksploatacyjną systemu RIS oraz Umową.

27) Generalny Wykonawca zobowiązany jest zapewnić w okresie gwarancji dostęp do aktualizacji oprogramowania, firmware, poprawek bezpieczeństwa, aktualizacji sygnatur, baz wiedzy, dokumentacji producentów, narzędzi diagnostycznych oraz innych elementów wymaganych dla bezpiecznej i prawidłowej eksploatacji dostarczonych rozwiązań, o ile są one właściwe dla danej kategorii produktu.

28) Aktualizacje oprogramowania, firmware, konfiguracji albo komponentów systemowych muszą być poprzedzone analizą wpływu na działanie systemu RIS, w szczególności na dostępność usług, bezpieczeństwo, integracje, transmisję danych, kompatybilność, monitoring techniczny, backup, replikację, dokumentację i możliwość odtworzenia stanu sprzed zmiany.

29) Aktualizacje i zmiany konfiguracyjne mogą być wykonywane wyłącznie w sposób kontrolowany, udokumentowany i zaakceptowany przez Zamawiającego, z zastrzeżeniem sytuacji awaryjnych określonych w Umowie albo procedurach eksploatacyjnych.

30) Generalny Wykonawca ponosi wszystkie koszty realizacji obowiązków gwarancyjnych, serwisowych i obsługi technicznej, w tym koszty robocizny, dojazdów, transportu, części, urządzeń zastępczych, wymiany, naprawy, diagnostyki, aktualizacji, testów, dokumentacji, wsparcia producentów i podwykonawców, o ile Umowa nie stanowi inaczej.

31) Generalny Wykonawca nie może odmówić wykonania obowiązków gwarancyjnych z powodu konieczności współpracy z producentem, podwykonawcą, operatorem telekomunikacyjnym, dostawcą Data Center, dostawcą licencji albo innym podmiotem, jeżeli dany element został dostarczony, wykonany, skonfigurowany, zintegrowany albo objęty odpowiedzialnością Generalnego Wykonawcy w ramach przedmiotu zamówienia.

32) Jeżeli usunięcie awarii, usterki, błędu, podatności albo niezgodności wymaga udziału producenta, autoryzowanego serwisu, dostawcy Data Center, operatora telekomunikacyjnego, dostawcy licencji, podwykonawcy albo innego podmiotu trzeciego, Generalny Wykonawca odpowiada za koordynację działań tych podmiotów oraz za doprowadzenie zgłoszenia do skutecznego zakończenia w zakresie objętym jego odpowiedzialnością.

33) Generalny Wykonawca zobowiązany jest zapewnić, aby czynności gwarancyjne i serwisowe wykonywane przez producentów, podwykonawców, dostawców albo inne podmioty trzecie były realizowane zgodnie z wymaganiami Zamawiającego dotyczącymi bezpieczeństwa, kontroli dostępu, poufności, logowania, dokumentowania czynności, uzgadniania prac oraz ochrony danych.

34) W przypadku stwierdzenia awarii powtarzalnych, problemów systemowych albo wad ujawniających się cyklicznie, Generalny Wykonawca zobowiązany jest przeprowadzić analizę przyczyn źródłowych oraz zaproponować i wdrożyć działania korygujące

i zapobiegawcze. Zakres i termin wykonania tych działań muszą być zgodne z Umową oraz uzgodnieniami z Zamawiającym.

35) Generalny Wykonawca zobowiązany jest zapewnić, aby realizacja obowiązków gwarancyjnych, serwisowych i SLA nie powodowała utraty gwarancji producentów, utraty wsparcia, naruszenia warunków licencyjnych, naruszenia zasad cyberbezpieczeństwa, obniżenia dostępności usług albo nieuzgodnionych zmian w konfiguracji systemu RIS.

36) Uprawnienia Zamawiającego wynikające z gwarancji nie wyłączają ani nie ograniczają uprawnień wynikających z rękojmi, Umowy, przepisów prawa, dokumentów gwarancyjnych producentów oraz innych wymagań określonych w PFU.

37) Niespełnienie parametrów SLA, brak skutecznej obsługi zgłoszeń, brak raportowania, brak aktualizacji dokumentacji, brak usunięcia wad albo powtarzające się awarie mogą stanowić podstawę do zastosowania środków przewidzianych w Umowie, w szczególności kar umownych, żądania działań naprawczych, eskalacji do producenta albo innych środków ochrony interesu Zamawiającego.

38) Zakończenie okresu gwarancji nie zwalnia Generalnego Wykonawcy z odpowiedzialności za wady zgłoszone w okresie gwarancji, nawet jeżeli ich usunięcie nastąpi po upływie tego okresu.

39) Przed zakończeniem okresu gwarancji Generalny Wykonawca zobowiązany jest, na żądanie Zamawiającego, przeprowadzić przegląd końcowy systemu RIS w zakresie objętym gwarancją. Przegląd końcowy powinien obejmować co najmniej ocenę stanu technicznego dostarczonych komponentów, aktualności dokumentacji, statusu zgłoszeń, statusu licencji i wsparcia producentów, statusu aktualizacji, statusu znanych problemów, poprawności monitoringu technicznego oraz rekomendacje dotyczące dalszego utrzymania systemu.

1.2.23. Przeglądy techniczne i aktualizacje oprogramowania w okresie gwarancji

1.2.23.1. Założenie ogólne

Generalny Wykonawca w okresie obowiązywania gwarancji zrealizuje usługę okresowych przeglądów technicznych, obsługi technicznej, konserwacji, aktualizacji oprogramowania oraz aktualizacji oprogramowania układowego dla zasobów infrastrukturalnych, sprzętowych, systemowych, aplikacyjnych i licencyjnych objętych jego odpowiedzialnością gwarancyjną.

Zakres usługi obejmuje wyłącznie komponenty, instalacje, urządzenia, systemy, oprogramowanie, konfiguracje, licencje i elementy integracyjne dostarczone, wykonane, zmodernizowane, rozbudowane, wymienione, skonfigurowane albo objęte przez Generalnego Wykonawcę odpowiedzialnością w ramach realizacji przedmiotu zamówienia.

Usługa nie obejmuje zasobów dostarczonych w ramach wcześniejszych etapów budowy lub rozbudowy systemu RIS, z zastrzeżeniem przypadków, w których Generalny Wykonawca w ramach realizacji przedmiotu zamówienia:

1) dokona ich modernizacji, wymiany, rozbudowy albo rekonfiguracji;

2) wykorzysta je jako element rozwiązania objętego własną odpowiedzialnością projektową, integracyjną lub gwarancyjną;
3) przejmie dla nich odpowiedzialność serwisową lub gwarancyjną na podstawie dokumentacji projektowej, oferty, umowy albo uzgodnienia zatwierdzonego przez Zamawiającego;
4) dokona ingerencji w sposób powodujący konieczność objęcia danego komponentu planem przeglądów, aktualizacji lub nadzoru technicznego.

Ostateczny zakres zasobów objętych usługą zostanie określony przez Generalnego Wykonawcę w dokumencie „Szczegółowy Plan Przeglądów i Aktualizacji” na podstawie przyjętego sposobu realizacji przedmiotu zamówienia, zatwierdzonej dokumentacji projektowej, dokumentacji powykonawczej, dokumentacji producentów, warunków gwarancji oraz uzgodnień dokonanych z Zamawiającym.

1.2.23.2. Obowiązek opracowania dokumentu

Generalny Wykonawca opracuje dokument pod nazwą „Szczegółowy Plan Przeglądów i Aktualizacji” i przekaże go Zamawiającemu do akceptacji przed przystąpieniem do Odbioru Końcowego.

Przekazanie Zamawiającemu zaakceptowanego „Szczegółowego Planu Przeglądów i Aktualizacji” stanowi warunek przystąpienia do Odbioru Końcowego. Brak dokumentu, brak kompletności dokumentu albo brak akceptacji Zamawiającego stanowi podstawę do odmowy rozpoczęcia procedury Odbioru Końcowego albo do wstrzymania tej procedury do czasu usunięcia braków.

Dokument musi odzwierciedlać rzeczywisty zakres rozwiązania wdrożonego przez Generalnego Wykonawcę. Dokument nie może stanowić wyłącznie powielenia dokumentacji z wcześniejszych etapów budowy lub rozbudowy systemu RIS.

1.2.23.3. Charakter dokumentu

„Szczegółowy Plan Przeglądów i Aktualizacji” będzie dokumentem wykonawczym i eksploatacyjnym określającym zasady utrzymania w okresie gwarancji tych elementów systemu RIS, za które odpowiada Generalny Wykonawca.

Dokument musi wskazywać:

1) jakie komponenty są objęte usługą;
2) jakie komponenty nie są objęte usługą, mimo ich współpracy z rozwiązaniem dostarczonym przez Generalnego Wykonawcę;
3) które komponenty istniejące zostały wykorzystane, zmodernizowane, rozbudowane, wymienione, skonfigurowane lub objęte integracją;

4) czy i w jakim zakresie ingerencja Generalnego Wykonawcy w komponent istniejący powoduje objęcie go odpowiedzialnością serwisową, gwarancyjną, aktualizacyjną lub przeglądową;
5) jakie czynności muszą być realizowane w okresie gwarancji dla utrzymania prawidłowego działania wdrożonego rozwiązania;
6) jaka jest częstotliwość tych czynności;
7) jakie raporty, protokoły i potwierdzenia będą przekazywane Zamawiającemu.

1.2.23.4. Minimalny zakres środowiska objętego analizą

Generalny Wykonawca w „Szczegółowym Planie Przeglądów i Aktualizacji” przeanalizuje co najmniej następujące kategorie zasobów, o ile wystąpią w przyjętym i zatwierdzonym sposobie realizacji przedmiotu zamówienia:

1) zasoby infrastruktury serwerowej, pamięci masowej, wirtualizacyjnej, kopii zapasowych i odtwarzania;
2) zasoby sieciowe, transmisyjne, radiowe, telekomunikacyjne i bezpieczeństwa teleinformatycznego;
3) zasoby zasilania podstawowego, gwarantowanego i awaryjnego;
4) wyposażenie techniczne pomieszczeń, szaf, punktów terenowych i obiektów infrastrukturalnych;
5) urządzenia i instalacje sensorowe;
6) urządzenia i instalacje systemu CCTV;
7) urządzenia i instalacje systemów VHF, AIS, DGNSS albo innych systemów radiokomunikacyjnych zastosowanych w rozwiązaniu;
8) urządzenia i instalacje hydrologiczne, meteorologiczne albo inne pomiarowe;
9) systemy antenowe, tory radiowe, tory kablowe, elementy montażowe i osprzęt instalacyjny;
10) oprogramowanie systemowe, narzędziowe, aplikacyjne, operatorskie, integracyjne, monitorujące i diagnostyczne;
11) oprogramowanie układowe urządzeń;
12) licencje, subskrypcje, certyfikaty, pakiety wsparcia producentów oraz uprawnienia do aktualizacji;
13) interfejsy integracyjne, konfiguracje, reguły, polityki, profile, konta techniczne i parametry pracy niezbędne do działania wdrożonego rozwiązania.

Wskazany katalog ma charakter ogólny i nie przesądza o zastosowaniu konkretnych technologii, producentów, urządzeń ani aplikacji. Ostateczny wykaz elementów zostanie określony przez Generalnego Wykonawcę na podstawie rzeczywiście wdrożonego i zatwierdzonego rozwiązania.

1.2.23.5. Wyłączenie zasobów historycznych

Generalny Wykonawca nie będzie zobowiązany do wykonywania przeglądów technicznych, konserwacji, aktualizacji ani obsługi technicznej zasobów dostarczonych w ramach wcześniejszych projektów, jeżeli zasoby te nie zostały objęte jego zakresem realizacji, ingerencji, modernizacji, rozbudowy, wymiany, konfiguracji, integracji lub odpowiedzialności gwarancyjnej.

Jeżeli rozwiązanie Generalnego Wykonawcy współpracuje z zasobami istniejącymi, „Szczegółowy Plan Przeglądów i Aktualizacji” musi jednoznacznie rozgraniczać:

1) zasoby objęte odpowiedzialnością Generalnego Wykonawcy;
2) zasoby istniejące wykorzystywane wyłącznie jako środowisko współpracy;
3) zasoby istniejące, do których Generalny Wykonawca wprowadził zmiany;
4) zasoby istniejące objęte odpowiedzialnością Generalnego Wykonawcy wyłącznie w zakresie dokonanej ingerencji;
5) zasoby wyłączone z usługi.

Rozgraniczenie musi być przedstawione w formie tabelarycznej i wymaga akceptacji Zamawiającego.

1.2.23.6. Wymagana zawartość dokumentu

„Szczegółowy Plan Przeglądów i Aktualizacji” musi zawierać co najmniej:

1) metrykę dokumentu, historię zmian oraz oznaczenie wersji;
2) podstawę opracowania dokumentu, w tym odniesienie do umowy, PFU, dokumentacji projektowej, dokumentacji powykonawczej, dokumentacji producentów, warunków gwarancji i zatwierdzonych uzgodnień z Zamawiającym;
3) opis okresu obowiązywania usługi;
4) opis zasad odpowiedzialności Generalnego Wykonawcy;
5) wykaz zasobów objętych usługą;
6) wykaz zasobów istniejących powiązanych funkcjonalnie lub technicznie z rozwiązaniem Generalnego Wykonawcy, lecz nieobjętych usługą;
7) wykaz zasobów istniejących objętych usługą w całości albo w ograniczonym zakresie;
8) wykaz lokalizacji, w których znajdują się zasoby objęte usługą;
9) wykaz oprogramowania objętego aktualizacją;
10) wykaz oprogramowania układowego objętego aktualizacją;
11) wykaz licencji, subskrypcji, certyfikatów i pakietów wsparcia wymaganych do realizacji usługi;
12) harmonogram przeglądów i aktualizacji;

13) zakres czynności dla poszczególnych kategorii zasobów;
14) zakres testów wykonywanych po przeglądach, aktualizacjach i interwencjach serwisowych;
15) procedury wykonywania kopii bezpieczeństwa przed aktualizacją lub zmianą konfiguracji;
16) procedury wycofania aktualizacji albo przywrócenia poprzedniego stanu działania;
17) zasady wykonywania prac bez naruszenia ciągłości działania systemu RIS;
18) wymagania dotyczące kwalifikacji personelu;
19) wykaz czynności wymagających udziału producenta, autoryzowanego partnera serwisowego albo osoby posiadającej wymagane uprawnienia;
20) zasady uzgadniania terminów prac z Zamawiającym;
21) zasady raportowania;
22) wzory protokołów, raportów i zestawień;
23) procedurę aktualizacji dokumentu.

1.2.23.7. Minimalna częstotliwość czynności

Generalny Wykonawca określi częstotliwość przeglądów, konserwacji, testów i aktualizacji na podstawie rodzaju zastosowanego rozwiązania, wymagań producentów, warunków gwarancji, wymagań bezpieczeństwa, dokumentacji technicznej oraz znaczenia danego komponentu dla ciągłości działania systemu RIS.

Harmonogram musi obejmować co najmniej:

1) czynności kwartalne;
2) czynności półroczne;
3) czynności roczne;
4) czynności doraźne po awarii, alarmie, interwencji serwisowej, zmianie konfiguracji, aktualizacji, wymianie urządzenia albo stwierdzeniu nieprawidłowości;
5) czynności wynikające z dokumentacji producenta, przepisów prawa, warunków gwarancji albo wymagań eksploatacyjnych.

Częstotliwość czynności nie może być mniejsza niż częstotliwość wymagana przez producenta, przepisy prawa, warunki gwarancji, warunki licencyjne albo dokumentację techniczną.

1.2.23.8. Zakres czynności serwisowych i obsługi technicznej

Zakres czynności zostanie określony przez Generalnego Wykonawcę odrębnie dla każdej kategorii zasobów objętych usługą. Minimalny zakres czynności obejmuje, adekwatnie do rodzaju komponentu:

1) kontrolę poprawności działania;
2) kontrolę stanu technicznego;
3) kontrolę parametrów pracy;
4) kontrolę alarmów, logów i zdarzeń;
5) kontrolę konfiguracji;
6) kontrolę dostępności usług;
7) kontrolę zasilania, transmisji, komunikacji i integracji;
8) czyszczenie, konserwację i wymianę elementów eksploatacyjnych;
9) testy eksploatacyjne i funkcjonalne;
10) testy mechanizmów redundancji, przełączenia awaryjnego i odtwarzania;
11) testy po aktualizacji lub zmianie konfiguracji;
12) kalibrację, wzorcowanie albo weryfikację urządzeń pomiarowych, jeżeli występują w rozwiązaniu;
13) wprowadzenie korekt zapewniających prawidłowe działanie zasobów objętych usługą;
14) sporządzenie protokołu z wykonanych czynności.

1.2.23.9. Aktualizacje oprogramowania

Generalny Wykonawca zapewni w okresie gwarancji dostęp do aktualizacji oprogramowania i oprogramowania układowego dla zasobów objętych usługą, w zakresie wynikającym z zastosowanego rozwiązania, warunków licencyjnych, warunków gwarancji, wymagań producentów oraz wymagań bezpieczeństwa.

Aktualizacje obejmują w szczególności:

1) poprawki bezpieczeństwa;
2) poprawki stabilności;
3) poprawki błędów;
4) aktualizacje wymagane do utrzymania kompatybilności;
5) aktualizacje wymagane do zachowania zgodności z dokumentacją producenta;
6) aktualizacje wymagane do prawidłowej współpracy komponentów objętych rozwiązaniem Generalnego Wykonawcy.

Przed wykonaniem aktualizacji Generalny Wykonawca musi:

1) zweryfikować zasadność aktualizacji;
2) zweryfikować kompatybilność aktualizacji z pozostałymi komponentami systemu;
3) ocenić wpływ aktualizacji na ciągłość działania systemu RIS;

4) wykonać kopię bezpieczeństwa konfiguracji, danych, maszyn wirtualnych albo innych zasobów, jeżeli aktualizacja może wpływać na ich działanie;
5) uzgodnić z Zamawiającym termin wykonania prac;
6) wykonać aktualizację w uzgodnionym oknie serwisowym;
7) przeprowadzić testy poaktualizacyjne;
8) sporządzić raport z aktualizacji.

Aktualizacja nie może powodować utraty danych, utraty konfiguracji, utraty licencji, ograniczenia funkcjonalności ani pogorszenia parametrów działania systemu. W przypadku niepowodzenia aktualizacji Generalny Wykonawca przywróci poprzedni stan działania albo wdroży inną procedurę naprawczą zaakceptowaną przez Zamawiającego.

1.2.23.10. Raportowanie

Generalny Wykonawca będzie raportował wykonanie usługi w cyklu kwartalnym. Raport kwartalny musi zawierać co najmniej:

1) wykaz wykonanych przeglądów;
2) wykaz wykonanych aktualizacji;
3) wykaz wykonanych czynności serwisowych i konserwacyjnych;
4) wykaz stwierdzonych usterek, alarmów, nieprawidłowości i odchyleń od parametrów wymaganych;
5) wykaz wykonanych działań naprawczych i prewencyjnych;
6) ocenę aktualności oprogramowania i oprogramowania układowego objętego usługą;
7) wykaz aktualizacji dostępnych, lecz niewdrożonych, wraz z uzasadnieniem;
8) informację o wpływie wykonanych czynności na ciągłość działania systemu;
9) rekomendacje dotyczące dalszych działań utrzymaniowych.

Jeżeli w ramach rozwiązania występują sensory, urządzenia pomiarowe albo wodowskazy objęte odpowiedzialnością Generalnego Wykonawcy, Generalny Wykonawca raz w roku sporządzi raport z poprawności ich działania oraz wykonania wymaganych kalibracji, wzorcowań albo weryfikacji pomiarowych.

Po każdej interwencji serwisowej Generalny Wykonawca sporządzi raport z interwencji zawierający co najmniej: datę i godzinę zgłoszenia, datę i godzinę rozpoczęcia prac, datę i godzinę zakończenia prac, opis przyczyny, opis wykonanych czynności, wykaz wymienionych elementów, wynik testów oraz informację o przywróceniu prawidłowego działania.

1.2.23.11. Aktualizacja dokumentu

Generalny Wykonawca zaktualizuje „Szczegółowy Plan Przeglądów i Aktualizacji” każdorazowo w przypadku:

1) zmiany zakresu zasobów objętych jego odpowiedzialnością;
2) zmiany konfiguracji systemu;
3) wymiany, rozbudowy, modernizacji albo usunięcia komponentu;
4) zmiany wersji oprogramowania lub oprogramowania układowego wpływającej na zasady utrzymania;
5) zmiany wymagań producenta;
6) zmiany warunków gwarancji, licencji, subskrypcji albo wsparcia technicznego;
7) zmiany lokalizacji komponentu;
8) zmiany sposobu integracji z zasobami istniejącymi;
9) stwierdzenia przez Zamawiającego niekompletności albo nieaktualności dokumentu.

Każda aktualizacja dokumentu musi zawierać historię zmian i wymaga akceptacji Zamawiającego.

1.2.23.12. Minimalne tabele wymagane w dokumencie

Generalny Wykonawca zamieści w „Szczegółowym Planie Przeglądów i Aktualizacji” co najmniej następujące zestawienia:

Tabela 1. Wykaz zasobów objętych usługą

Lp.	Nazwa zasobu	Kategoria zasobu	Lokalizacja	Sposób powstania odpowiedzialności Generalnego Wykonawcy	Zakres odpowiedzialności	Typ czynności	Częstotliwość	Uwagi

Tabela 2. Wykaz zasobów istniejących powiązanych z rozwiązaniem, lecz nieobjętych usługą

Lp.	Nazwa zasobu istniejącego	Lokalizacja	Rola w systemie	Powiązanie z rozwiązaniem Generalnego Wykonawcy	Zakres wyłączenia	Uzasadnienie wyłączenia	Uwagi

Tabela 3. Wykaz oprogramowania i oprogramowania układowego objętego aktualizacją

Lp.	Nazwa oprogramowania / firmware	Producent	Wersja bazowa	Miejsce instalacji	Powiązany komponent	Zakres aktualizacji	Częstotliwość weryfikacji	Uwagi

Tabela 4. Harmonogram czynności przeglądowych, serwisowych i aktualizacyjnych

Lp.	Zasób / grupa zasobów	Zakres czynności	Częstotliwość	Wymagany personel / uprawnienia	Wymagany dokument potwierdzający	Uwagi

Tabela 5. Wykaz lokalizacji objętych usługą

Lp.	Lokalizacja	Typ obiektu	Zasoby objęte usługą	Zasoby istniejące nieobjęte usługą	Wymagania dostępu	Uwagi

1.2.23.13. Warunki akceptacji dokumentu

Zamawiający zaakceptuje „Szczegółowy Plan Przeglądów i Aktualizacji” po potwierdzeniu, że dokument:

1) obejmuje wszystkie zasoby objęte odpowiedzialnością Generalnego Wykonawcy;
2) jednoznacznie rozgranicza zasoby objęte usługą i zasoby wyłączone z usługi;
3) wskazuje wpływ wykorzystania zasobów istniejących na zakres odpowiedzialności Generalnego Wykonawcy;
4) określa częstotliwość i zakres czynności dla poszczególnych kategorii zasobów;
5) określa zasady aktualizacji oprogramowania i oprogramowania układowego;
6) określa zasady raportowania;
7) zawiera wymagane tabele i wzory dokumentów;
8) uwzględnia wymagania producentów, warunki gwarancji, warunki licencyjne i wymagania bezpieczeństwa;
9) zapewnia możliwość weryfikacji wykonania obowiązków gwarancyjnych;
10) jest spójny z dokumentacją projektową, dokumentacją powykonawczą oraz rzeczywistym zakresem wdrożenia.

1.2.24. Usługa Utrzymania

1) Wykonawca zobowiązany jest do świadczenia Usługi Utrzymania jako usługi odrębnej od świadczeń gwarancyjnych, ukierunkowanej na utrzymanie odporności Systemu na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych oraz usług realizowanych przez System RIS.
2) Usługa Utrzymania stanowi element Przedmiotu Zamówienia i obejmuje współpracę z Zamawiającym w sposób umożliwiający Zamawiającemu wywiązywanie się z obowiązków wynikających z ustawy o krajowym systemie cyberbezpieczeństwa, właściwych dla operatora usługi kluczowej oraz podmiotu kluczowego.
3) W ramach Usługi Utrzymania Wykonawca zapewni ciągłość i bezpieczeństwo łańcucha dostaw produktów ICT, usług ICT i procesów ICT wykorzystywanych w Systemie. Wykonawca zobowiązany jest do nałożenia na swoich poddostawców obowiązków w zakresie cyberbezpieczeństwa odpowiadających obowiązkom Wykonawcy, w szczególności w zakresie niezwłocznego zgłaszania podatności oraz wsparcia w obsłudze incydentów.
4) Wykonawca wyznaczy dedykowanego specjalistę ds. cyberbezpieczeństwa pełniącego rolę koordynatora Usługi Utrzymania, odpowiedzialnego za bieżący kontakt z Zamawiającym w obszarze bezpieczeństwa informacji. Dane tej osoby muszą zostać przekazane Zamawiającemu najpóźniej przed rozpoczęciem świadczenia Usługi Utrzymania.

5) Wykonawca gwarantuje, że osoby, w tym pracownicy poddostawców, którym powierzono realizację zadań w zakresie bezpieczeństwa Systemu, posiadają wymagane kwalifikacje oraz nie były karane za przestępstwa przeciwko ochronie informacji. Na żądanie Zamawiającego Wykonawca przedstawi aktualną informację z Krajowego Rejestru Karnego dla wskazanych osób.

6) Wykonawca odpowiada za bieżące monitorowanie podatności bezpieczeństwa dotyczących Oprogramowania, Infrastruktury oraz produktów i usług dostawców zewnętrznych użytych w Systemie, w tym z wykorzystaniem publicznych baz podatności, w szczególności CVE. Wykonawca zobowiązany jest informować Zamawiającego o konieczności wdrożenia poprawek bezpieczeństwa lub innych działań ograniczających ryzyko nie później niż w terminie 24 godzin od publikacji informacji o podatności krytycznej.

7) W przypadku wystąpienia incydentu bezpieczeństwa dotyczącego Systemu, Wykonawca zobowiązany jest do współpracy z Zamawiającym przy jego analizie, ograniczeniu skutków, usunięciu przyczyn oraz odtworzeniu bezpiecznego stanu pracy Systemu. Wykonawca przekaże Zamawiającemu dane niezbędne do dokonania zgłoszenia incydentu do właściwego CSIRT nie później niż w terminie 24 godzin od wykrycia incydentu albo od uzyskania informacji o jego wystąpieniu.

8) Wykonawca zobowiązany jest niezwłocznie informować Zamawiającego o każdej zmianie w łańcuchu dostaw, która może skutkować wprowadzeniem do Systemu rozwiązań pochodzących od dostawców wysokiego ryzyka. W takim przypadku Zamawiający będzie uprawniony do żądania zastąpienia takich komponentów na koszt Wykonawcy.

9) Zamawiający ma prawo przeprowadzania audytów bezpieczeństwa systemu RIS oraz komponentów, usług, konfiguracji, interfejsów i dokumentacji objętych przedmiotem zamówienia. Generalny Wykonawca zobowiązany jest do pełnej współpracy przy audycie, w szczególności do udostępnienia informacji, dokumentów, logów, konfiguracji, skryptów, kodów źródłowych komponentów wytworzonych albo zmodyfikowanych przez Generalnego Wykonawcę, dokumentacji technicznej oraz innych materiałów niezbędnych do oceny bezpieczeństwa systemu RIS, a także do usuwania stwierdzonych podatności, niezgodności i błędów konfiguracyjnych w zakresie swojej odpowiedzialności.

10) Wykonawca zobowiązany jest do sporządzania i przekazywania Zamawiającemu raportu kwartalnego dotyczącego bezpieczeństwa Systemu nie rzadziej niż raz na kwartał, w terminie do 10. dnia roboczego po zakończeniu danego kwartału.

11) Raport kwartalny musi zawierać co najmniej:

    1) zestawienie incydentów i zdarzeń bezpieczeństwa;

    2) zestawienie podatności wraz ze stanem ich obsługi;

    3) informację o wdrożonych poprawkach bezpieczeństwa i zmianach konfiguracyjnych;

    4) status rekomendacji z audytów i testów;

    5) informacje o zmianach w łańcuchu dostaw;

    6) wyniki pomiaru SLA;

    7) wykaz przekroczeń SLA i działań korygujących;

    8) ocenę trendów ryzyka i rekomendacje działań prewencyjnych.

12) Minimalne wymagania SLA dla Usługi Utrzymania obejmują co najmniej:

1) przekazanie informacji o podatności krytycznej – do 24 godzin od publikacji informacji o podatności;

2) przekazanie danych niezbędnych do zgłoszenia incydentu do właściwego CSIRT – do 24 godzin od wykrycia incydentu albo uzyskania informacji o jego wystąpieniu;

3) przekazanie raportu kwartalnego – do 10. dnia roboczego po zakończeniu kwartału.

13) Usługa Utrzymania podlega odbiorowi na podstawie spełnienia wymagań określonych w PFU, SWZ, Umowie, dotrzymania parametrów SLA oraz prawidłowości i kompletności raportów kwartalnych oraz innych materiałów przekazywanych przez Wykonawcę w okresie świadczenia usługi. Końcowe potwierdzenie należytego wykonania Usługi Utrzymania następuje w ramach odbioru …….

1.2.25. Ogólne wymagania dotyczące przedmiotu dostaw realizowanych przez Generalnego Wykonawcę

Wszystkie urządzenia, sprzęt, komponenty techniczne, elementy infrastruktury, oprogramowanie standardowe, licencje, subskrypcje, moduły, akcesoria, części, materiały instalacyjne oraz inne elementy dostarczane przez Generalnego Wykonawcę w ramach realizacji przedmiotu zamówienia muszą być fabrycznie nowe, pełnowartościowe, nieużywane, wolne od wad fizycznych i prawnych, kompletne, dopuszczone do obrotu i eksploatacji oraz zgodne z wymaganiami PFU, dokumentacji projektowej, dokumentów branżowych, obowiązujących przepisów prawa, norm, standardów i zaleceń producentów.

Wymaganie fabrycznej nowości dotyczy w szczególności urządzeń serwerowych, macierzy dyskowych, przełączników, routerów, urządzeń transmisyjnych, urządzeń radiokomunikacyjnych, kamer, rejestratorów, sensorów, czujników, sterowników, zasilaczy, modułów bateryjnych, szaf teletechnicznych, urządzeń monitoringu środowiskowego, urządzeń kontroli dostępu, urządzeń bezpieczeństwa, urządzeń sieciowych, wkładek optycznych, kabli, modułów rozszerzeń, kart, adapterów, nośników danych, elementów montażowych oraz pozostałych komponentów mających wpływ na działanie systemu RIS.

Dostarczane urządzenia i komponenty muszą pochodzić z autoryzowanego krajowego kanału sprzedaży producenta albo autoryzowanego partnera producenta. Generalny Wykonawca zobowiązany jest, na żądanie Zamawiającego, przedstawić dokumenty potwierdzające legalne pochodzenie dostarczanych produktów, uprawnienie do ich sprzedaży, objęcie ich gwarancją producenta, wsparciem producenta oraz prawem do korzystania z wymaganych licencji, subskrypcji, aktualizacji i usług serwisowych.

Nie dopuszcza się dostarczania urządzeń, oprogramowania, licencji albo komponentów pochodzących z rynku wtórnego, odnowionych, regenerowanych, powystawowych, rekondycjonowanych, demonstracyjnych, używanych, wycofanych z wcześniejszej eksploatacji, pochodzących z demontażu albo nieobjętych pełnym wsparciem producenta, chyba że Zamawiający wyrazi na to uprzednią pisemną zgodę w odniesieniu do konkretnego elementu i z uzasadnieniem technicznym.

Dostarczane urządzenia, sprzęt i komponenty muszą być przeznaczone do pracy w środowisku odpowiadającym ich funkcji i miejscu instalacji. W szczególności:

1) komponenty instalowane w centrum przetwarzania danych, serwerowni głównej, ośrodku zapasowym albo szafach RACK muszą być przeznaczone do pracy ciągłej w środowisku centrum przetwarzania danych albo środowisku serwerowym;
2) komponenty instalowane w szafach teletechnicznych typu zewnętrznego muszą być przystosowane do pracy w warunkach terenowych, w zakresie temperatur, wilgotności, zapylenia, wibracji i oddziaływań środowiskowych właściwych dla danej lokalizacji;
3) urządzenia instalowane na obiektach wieżowych, mostowych, hydrotechnicznych, słupach, konstrukcjach wsporczych albo w lokalizacjach nadwodnych muszą być przystosowane do pracy w warunkach zewnętrznych, podwyższonej wilgotności, promieniowania UV, zmiennych temperatur, wiatru, oblodzenia, drgań i zwiększonej korozyjności środowiska;
4) urządzenia radiokomunikacyjne, transmisyjne, antenowe, pomiarowe i obserwacyjne muszą być zgodne z wymaganiami środowiskowymi, elektromagnetycznymi, zasilającymi, montażowymi i eksploatacyjnymi właściwymi dla ich przeznaczenia;
5) oprogramowanie standardowe, licencje, subskrypcje i komponenty programowe muszą być przeznaczone do pracy produkcyjnej, objęte prawem do użytkowania przez Zamawiającego i możliwe do utrzymania w okresie wymaganym w PFU oraz umowie.

Wszystkie dostarczane komponenty muszą być kompletne pod względem sprzętowym, programowym, licencyjnym, montażowym, instalacyjnym, konfiguracyjnym, serwisowym i eksploatacyjnym. Dostawa musi obejmować wszystkie elementy niezbędne do prawidłowego montażu, uruchomienia, konfiguracji, integracji, monitorowania, zarządzania, utrzymania i eksploatacji danego rozwiązania, w tym w szczególności przewody, wkładki, moduły, adaptery, karty rozszerzeń, szyny, uchwyty, półki, elementy montażowe, zasilacze, licencje, subskrypcje, aktywacje funkcji, certyfikaty, klucze licencyjne, konta techniczne, dokumentację, narzędzia administracyjne i oprogramowanie zarządzające.

Brak wskazania w PFU konkretnego elementu pomocniczego, akcesorium, licencji, modułu, przewodu, wkładki, aktywacji funkcji albo komponentu pośredniego nie zwalnia Generalnego Wykonawcy z obowiązku jego dostarczenia, jeżeli jest on niezbędny do osiągnięcia wymaganej funkcjonalności, wydajności, dostępności, bezpieczeństwa, interoperacyjności, monitorowania, serwisowania albo zgodności z wymaganiami producenta.

Dostarczane urządzenia i oprogramowanie muszą być objęte gwarancją oraz wsparciem producenta przez okres nie krótszy niż wymagany w PFU i umowie. Wsparcie producenta musi obejmować co najmniej dostęp do aktualizacji oprogramowania, firmware, poprawek bezpieczeństwa, baz wiedzy, dokumentacji technicznej, narzędzi diagnostycznych, zgłoszeń serwisowych oraz obsługi gwarancyjnej, o ile taki zakres jest właściwy dla danej kategorii produktu.

Nie dopuszcza się dostarczania komponentów, które na dzień złożenia oferty albo dostawy znajdują się w fazie zakończenia sprzedaży, zakończenia wsparcia, zakończenia rozwoju, zakończenia dostępności części zamiennych albo dla których producent ogłosił datę wycofania

wsparcia przypadającą przed zakończeniem okresu gwarancji lub wymaganego okresu utrzymania, chyba że Zamawiający wyrazi na to uprzednią pisemną zgodę.

Generalny Wykonawca zobowiązany jest zapewnić kompatybilność wszystkich dostarczanych komponentów z docelową architekturą systemu RIS, istniejącymi zasobami Zamawiającego wykorzystywanymi w ramach zamówienia, wymaganiami integracyjnymi, wymaganiami cyberbezpieczeństwa, wymaganiami monitoringu technicznego, wymaganiami zasilania, transmisji danych, warunkami środowiskowymi oraz dokumentacją producentów. Kompatybilność ta musi zostać potwierdzona w dokumentacji projektowej, a w przypadku komponentów infrastrukturalnych również przez odniesienie do list kompatybilności producentów, jeżeli takie listy są publikowane.

W przypadku urządzeń infrastrukturalnych, serwerowych, sieciowych, pamięci masowej, bezpieczeństwa, backupu, transmisji danych, CCTV, VHF/AIS/DGNSS, sensorów, zasilania awaryjnego i monitoringu technicznego Generalny Wykonawca zobowiązany jest zapewnić możliwość objęcia ich monitoringiem technicznym systemu RIS, odczytu podstawowych parametrów pracy, alarmów, stanu dostępności, stanu połączeń, stanu zasilania, stanu środowiskowego albo innych parametrów właściwych dla danej klasy urządzeń.

Dostarczane komponenty muszą być możliwe do bezpiecznego administrowania i utrzymania przez Zamawiającego. Wymaga się w szczególności możliwości zmiany domyślnych poświadczeń, nadawania uprawnień, wykonywania kopii konfiguracji, odtwarzania konfiguracji po awarii, aktualizacji oprogramowania lub firmware, monitorowania stanu, rejestrowania zdarzeń oraz integracji z przyjętym modelem zarządzania i utrzymania systemu RIS.

Wszystkie dostarczane urządzenia, systemy, aplikacje, licencje i komponenty programowe muszą zostać przekazane Zamawiającemu wraz z kompletną dokumentacją techniczną, eksploatacyjną, licencyjną, gwarancyjną i serwisową. Dokumentacja musi obejmować co najmniej karty katalogowe, instrukcje instalacji, instrukcje konfiguracji, instrukcje administracyjne, instrukcje eksploatacyjne, warunki gwarancji, informacje o wsparciu producenta, wykaz licencji, numery seryjne, numery kontraktów serwisowych, wersje oprogramowania, wersje firmware oraz informacje wymagane do późniejszego utrzymania i rozbudowy systemu.

Generalny Wykonawca zobowiązany jest przed dostawą przedstawić Zamawiającemu do akceptacji wykaz planowanych dostaw, obejmujący co najmniej nazwę kategorii komponentu, producenta, model albo typ, ilość, podstawowe parametry techniczne, miejsce instalacji, przeznaczenie, wymagane licencje, wymagany okres gwarancji i wsparcia, przewidywany sposób integracji z systemem RIS oraz odniesienie do wymagań PFU, które dany komponent realizuje.

Zamawiający może odmówić akceptacji dostawy komponentu, jeżeli nie spełnia on wymagań PFU, nie jest zgodny z zaakceptowaną dokumentacją projektową, nie pochodzi z autoryzowanego krajowego kanału sprzedaży, nie jest objęty wymaganym wsparciem producenta, jest niekompletny, znajduje się poza okresem aktywnego wsparcia producenta, nie jest kompatybilny z docelową architekturą albo jego zastosowanie mogłoby negatywnie wpłynąć na bezpieczeństwo, niezawodność, dostępność, interoperacyjność, utrzymanie lub rozwój systemu RIS.

Wszystkie dostarczone komponenty muszą zostać ujęte w dokumentacji powykonawczej, dokumentacji eksploatacyjnej, wykazie zasobów systemu RIS, dokumentacji licencyjnej,

dokumentacji gwarancyjnej oraz systemie monitorowania zasobów, jeżeli dany komponent podlega monitorowaniu. Dokumentacja musi umożliwiać jednoznaczną identyfikację komponentu, jego lokalizacji, konfiguracji, wersji, numeru seryjnego, okresu gwarancji, okresu wsparcia, powiązań z innymi komponentami oraz odpowiedzialności serwisowej.

2. Część informacyjna

2.1. Przepisy prawne, normy i standardy związane z projektowaniem i wykonaniem zamierzenia inwestycyjnego

Wykaz zamieszczony w niniejszym rozdziale obejmuje akty prawne, akty normatywne, normy, standardy i pozostałe dokumenty odniesienia właściwe dla projektowania, wykonania, uruchomienia, odbioru i przekazania do eksploatacji elementów systemu RIS w formule „zaprojektuj i zbuduj”. Wykaz zachowuje układ kategorii właściwy dla części informacyjnej PFU, z podziałem na przepisy Unii Europejskiej, umowy międzynarodowe, przepisy krajowe rangi ustawowej i wykonawczej, prawo miejscowe, normy i standardy techniczne oraz pozostałe dokumenty programowe i techniczne.

Uwaga:

Niewyszczególnienie w niniejszym dokumencie jakichkolwiek z obowiązujących aktów prawnych, aktów normatywnych lub standardów nie zwalnia Generalnego Wykonawcy z obowiązku ich stosowania.

2.1.1. Przepisy prawne Unii Europejskiej

2.1.1.1. Usługi informacji rzecznej RIS, żegluga śródlądowa i sieć TEN-T

1) Dyrektywa 2005/44/WE Parlamentu Europejskiego i Rady z dnia 7 września 2005 r. w sprawie zharmonizowanych usług informacji rzecznej (RIS) na śródlądowych drogach wodnych we Wspólnocie, Dz. Urz. UE L 255 z 30.09.2005, s. 152, w brzmieniu skonsolidowanym obowiązującym od 1.01.2026 r.
2) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2025/2482 z dnia 26 listopada 2025 r. zmieniająca dyrektywę 2005/44/WE w sprawie zharmonizowanych usług informacji rzecznej (RIS) na śródlądowych drogach wodnych we Wspólnocie, Dz. Urz. UE L, 2025/2482, 12.12.2025.
3) Rozporządzenie Komisji (WE) nr 414/2007 z dnia 13 marca 2007 r. w sprawie wytycznych technicznych dotyczących planowania, wdrażania i wykorzystania operacyjnego usług informacji rzecznej (RIS), Dz. Urz. UE L 105 z 23.04.2007, s. 1.
4) Rozporządzenie Komisji (WE) nr 416/2007 z dnia 22 marca 2007 r. dotyczące specyfikacji technicznych komunikatów dla kierowników statków, Dz. Urz. UE L 105 z 23.04.2007, s. 88, w brzmieniu wynikającym z rozporządzenia wykonawczego Komisji (UE) 2018/2032, Dz. Urz. UE L 332 z 28.12.2018, s. 1.

5) Rozporządzenie wykonawcze Komisji (UE) nr 909/2013 z dnia 10 września 2013 r. w sprawie specyfikacji technicznych systemu obrazowania elektronicznych map nawigacyjnych i informacji dla żeglugi śródlądowej (Inland ECDIS), Dz. Urz. UE L 258 z 28.09.2013, s. 1.
6) Rozporządzenie wykonawcze Komisji (UE) 2019/838 z dnia 20 lutego 2019 r. w sprawie specyfikacji technicznych systemów śledzenia i namierzania statków oraz uchylające rozporządzenie Komisji (WE) nr 415/2007, Dz. Urz. UE L 138 z 24.05.2019, s. 31.
7) Rozporządzenie wykonawcze Komisji (UE) 2019/1744 z dnia 17 września 2019 r. w sprawie specyfikacji technicznych elektronicznego raportowania statków w żegludze śródlądowej oraz uchylające rozporządzenie Komisji (UE) nr 164/2010, Dz. Urz. UE L 273 z 25.10.2019, s. 1.
8) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1629 z dnia 14 września 2016 r. ustanawiająca wymagania techniczne dla statków żeglugi śródlądowej, Dz. Urz. UE L 252 z 16.09.2016, s. 118.
9) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1679 z dnia 13 czerwca 2024 r. w sprawie unijnych wytycznych dotyczących rozwoju transeuropejskiej sieci transportowej, Dz. Urz. UE L, 2024/1679, 28.06.2024.
10) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1315/2013 z dnia 11 grudnia 2013 r. w sprawie unijnych wytycznych dotyczących rozwoju transeuropejskiej sieci transportowej, Dz. Urz. UE L 348 z 20.12.2013, s. 1, w zakresie przepisów przejściowych i odniesień historycznych.

2.1.1.2. Usługi cyfrowe, dane, cyberbezpieczeństwo, interoperacyjność i dostępność

W zakresie projektowania, wykonania, wdrożenia, utrzymania i rozwoju usług cyfrowych, aplikacji, portali, interfejsów użytkownika, interfejsów integracyjnych, API, przetwarzania danych, cyberbezpieczeństwa, interoperacyjności oraz dostępności cyfrowej zastosowanie mają w szczególności następujące akty prawa Unii Europejskiej:

1) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/2102 z dnia 26 października 2016 r. w sprawie dostępności stron internetowych i mobilnych aplikacji organów sektora publicznego, Dz. Urz. UE L 327 z 02.12.2016, s. 1, z późniejszymi zmianami — w zakresie zapewnienia dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów sektora publicznego, w tym zasad projektowania, budowy, utrzymania i aktualizacji rozwiązań cyfrowych.
2) Decyzja wykonawcza Komisji (UE) 2018/1523 z dnia 11 października 2018 r. ustanawiająca wzór oświadczenia w sprawie dostępności zgodnie z dyrektywą Parlamentu Europejskiego i Rady (UE) 2016/2102 w sprawie dostępności stron internetowych i mobilnych aplikacji organów sektora publicznego, Dz. Urz. UE L 256 z 12.10.2018, s. 103 — w zakresie informacji niezbędnych do przygotowania, aktualizacji i publikacji deklaracji dostępności dla publicznie udostępnianych stron internetowych, portali, aplikacji mobilnych i usług cyfrowych.

3) Decyzja wykonawcza Komisji (UE) 2018/1524 z dnia 11 października 2018 r. ustanawiająca metodykę monitorowania i zasady przekazywania przez państwa członkowskie sprawozdań zgodnie z dyrektywą Parlamentu Europejskiego i Rady (UE) 2016/2102 w sprawie dostępności stron internetowych i mobilnych aplikacji organów sektora publicznego, Dz. Urz. UE L 256 z 12.10.2018, s. 108 — w zakresie metodyki oceny i monitorowania zgodności stron internetowych i aplikacji mobilnych z wymaganiami dostępności cyfrowej.

4) Decyzja wykonawcza Komisji (UE) 2018/2048 z dnia 20 grudnia 2018 r. w sprawie zharmonizowanej normy dotyczącej stron internetowych i aplikacji mobilnych opracowanej na potrzeby dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/2102, Dz. Urz. UE L 327 z 21.12.2018, s. 84, z późniejszymi zmianami — w zakresie wskazania normy zharmonizowanej służącej ocenie zgodności wymagań dostępności cyfrowej.

5) Decyzja wykonawcza Komisji (UE) 2021/1339 z dnia 11 sierpnia 2021 r. zmieniająca decyzję wykonawczą (UE) 2018/2048 w odniesieniu do zharmonizowanej normy dotyczącej stron internetowych i aplikacji mobilnych, Dz. Urz. UE L 289 z 12.08.2021, s. 53 — w zakresie odniesienia do normy EN 301 549 V3.2.1 albo jej aktualnej wersji zharmonizowanej właściwej dla danego zakresu rozwiązań ICT.

6) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/882 z dnia 17 kwietnia 2019 r. w sprawie wymogów dostępności produktów i usług, Dz. Urz. UE L 151 z 07.06.2019, s. 70, z późniejszymi zmianami — w zakresie wymagań dostępności dla produktów i usług objętych zakresem dyrektywy, jeżeli dostarczane w ramach zamówienia produkty, usługi, komponenty aplikacyjne, interfejsy lub usługi cyfrowe mieszczą się w jej zakresie zastosowania.

7) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/903 z dnia 13 marca 2024 r. w sprawie ustanowienia środków na rzecz wysokiego poziomu interoperacyjności sektora publicznego w całej Unii, Dz. Urz. UE L 2024/903 z 22.03.2024 — w zakresie interoperacyjności transgranicznych usług cyfrowych sektora publicznego, oceny interoperacyjności, rozwiązań interoperacyjnych oraz ponownego wykorzystania rozwiązań wspierających świadczenie usług publicznych drogą elektroniczną.

8) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z dnia 30 maja 2022 r. w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724, Dz. Urz. UE L 152 z 03.06.2022, s. 1 — w zakresie zarządzania danymi, ponownego wykorzystywania niektórych kategorii danych oraz zasad udostępniania danych w ekosystemach danych, jeżeli wymagania te mają zastosowanie do danych przetwarzanych lub udostępnianych przez system RIS.

9) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/2854 z dnia 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz zmieniające rozporządzenie (UE) 2017/2394 i dyrektywę (UE) 2020/1828, Dz. Urz. UE L 2023/2854 z 22.12.2023 — w zakresie zasad dostępu do danych, udostępniania danych, interoperacyjności i przenoszalności danych, jeżeli wymagania te mają zastosowanie do danych, urządzeń, usług lub komponentów dostarczanych w ramach zamówienia.

10) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1724 z dnia 2 października 2018 r. w sprawie utworzenia jednolitego portalu cyfrowego w celu zapewnienia dostępu do informacji, procedur oraz usług wsparcia i rozwiązywania problemów oraz zmieniające

rozporządzenie (UE) nr 1024/2012, Dz. Urz. UE L 295 z 21.11.2018, s. 1 — w zakresie zasad świadczenia usług cyfrowych, dostępności informacji i procedur oraz wymagań dotyczących interoperacyjności usług publicznych, jeżeli zakres ten ma zastosowanie do usług cyfrowych realizowanych w ramach systemu RIS.

11) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji oraz zmieniające określone akty ustawodawcze Unii, Dz. Urz. UE L 2024/1689 z 12.07.2024 — w zakresie, w jakim dostarczane rozwiązania aplikacyjne, moduły analityczne, komponenty automatyzacji albo usługi cyfrowe będą wykorzystywać systemy sztucznej inteligencji lub funkcje mogące podlegać wymaganiom tego rozporządzenia.

12) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, Dz. Urz. UE L 119 z 04.05.2016, s. 1, z późniejszymi zmianami — w zakresie ochrony danych osobowych przetwarzanych w systemach, usługach cyfrowych, interfejsach użytkownika, API, logach, mechanizmach kontroli dostępu, integracjach i dokumentacji systemu RIS.

13) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148, Dz. Urz. UE L 333 z 27.12.2022, s. 80 — w zakresie wymagań cyberbezpieczeństwa, zarządzania ryzykiem, obsługi incydentów, ciągłości działania oraz bezpieczeństwa sieci i systemów informatycznych, jeżeli wymagania te mają zastosowanie do systemu RIS albo podmiotów uczestniczących w jego eksploatacji.

14) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE, Dz. Urz. UE L 257 z 28.08.2014, s. 73, z późniejszymi zmianami — w zakresie identyfikacji elektronicznej, usług zaufania, podpisów elektronicznych, pieczęci elektronicznych, znaczników czasu, uwierzytelniania i integralności dokumentów elektronicznych, jeżeli rozwiązania systemu RIS będą wykorzystywać takie mechanizmy.

15) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. zmieniające rozporządzenie (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej, Dz. Urz. UE L 2024/1183 z 30.04.2024 — w zakresie, w jakim rozwiązania cyfrowe, usługi elektroniczne, mechanizmy uwierzytelniania albo integracje systemu RIS będą wykorzystywać rozwiązania identyfikacji elektronicznej lub europejskie ramy tożsamości cyfrowej.

2.1.1.3. Wyroby, urządzenia, kompatybilność elektromagnetyczna i wymagania produktowe

1) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 305/2011 z dnia 9 marca 2011 r. ustanawiające zharmonizowane warunki wprowadzania do obrotu wyrobów

budowlanych i uchylające dyrektywę Rady 89/106/EWG, Dz. Urz. UE L 88 z 4.04.2011, s. 5.

2) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/3110 z dnia 27 listopada 2024 r. ustanawiające zharmonizowane przepisy dotyczące wprowadzania do obrotu wyrobów budowlanych i uchylające rozporządzenie (UE) nr 305/2011, Dz. Urz. UE L, 2024/3110, 18.12.2024, w zakresie terminów stosowania przepisów i okresów przejściowych.
3) Dyrektywa Parlamentu Europejskiego i Rady 2014/53/UE z dnia 16 kwietnia 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich dotyczących udostępniania na rynku urządzeń radiowych, Dz. Urz. UE L 153 z 22.05.2014, s. 62.
4) Dyrektywa Parlamentu Europejskiego i Rady 2014/30/UE z dnia 26 lutego 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do kompatybilności elektromagnetycznej, Dz. Urz. UE L 96 z 29.03.2014, s. 79.
5) Dyrektywa Parlamentu Europejskiego i Rady 2014/35/UE z dnia 26 lutego 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do udostępniania na rynku sprzętu elektrycznego przewidzianego do stosowania w określonych granicach napięcia, Dz. Urz. UE L 96 z 29.03.2014, s. 357.
6) Dyrektywa Parlamentu Europejskiego i Rady 2011/65/UE z dnia 8 czerwca 2011 r. w sprawie ograniczenia stosowania niektórych niebezpiecznych substancji w sprzęcie elektrycznym i elektronicznym, Dz. Urz. UE L 174 z 1.07.2011, s. 88.
7) Dyrektywa Parlamentu Europejskiego i Rady 2012/19/UE z dnia 4 lipca 2012 r. w sprawie zużytego sprzętu elektrycznego i elektronicznego, Dz. Urz. UE L 197 z 24.07.2012, s. 38.
8) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1542 z dnia 12 lipca 2023 r. w sprawie baterii i zużytych baterii, Dz. Urz. UE L 191 z 28.07.2023, s. 1.
9) Dyrektywa Parlamentu Europejskiego i Rady 2006/42/WE z dnia 17 maja 2006 r. w sprawie maszyn, Dz. Urz. UE L 157 z 9.06.2006, s. 24.
10) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1230 z dnia 14 czerwca 2023 r. w sprawie maszyn i uchylające dyrektywę 2006/42/WE oraz dyrektywę Rady 73/361/EWG, Dz. Urz. UE L 165 z 29.06.2023, s. 1, w zakresie terminów stosowania i okresów przejściowych.
11) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1781 z dnia 13 czerwca 2024 r. ustanawiające ramy ustalania wymogów ekoprojektu dla zrównoważonych produktów, Dz. Urz. UE L, 2024/1781, 28.06.2024.

2.1.1.4. Środowisko, gospodarka wodna, oceny oddziaływania i finansowanie UE

1) Dyrektywa 2000/60/WE Parlamentu Europejskiego i Rady z dnia 23 października 2000 r. ustanawiająca ramy wspólnotowego działania w dziedzinie polityki wodnej, Dz. Urz. WE L 327 z 22.12.2000, s. 1.

2) Dyrektywa Parlamentu Europejskiego i Rady 2011/92/UE z dnia 13 grudnia 2011 r. w sprawie oceny skutków wywieranych przez niektóre przedsięwzięcia publiczne i prywatne na środowisko, Dz. Urz. UE L 26 z 28.01.2012, s. 1.
3) Dyrektywa Parlamentu Europejskiego i Rady 2014/52/UE z dnia 16 kwietnia 2014 r. zmieniająca dyrektywę 2011/92/UE, Dz. Urz. UE L 124 z 25.04.2014, s. 1.
4) Dyrektywa Parlamentu Europejskiego i Rady 2009/147/WE z dnia 30 listopada 2009 r. w sprawie ochrony dzikiego ptactwa, Dz. Urz. UE L 20 z 26.01.2010, s. 7.
5) Dyrektywa Rady 92/43/EWG z dnia 21 maja 1992 r. w sprawie ochrony siedlisk przyrodniczych oraz dzikiej fauny i flory, Dz. Urz. WE L 206 z 22.07.1992, s. 7.
6) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2020/852 z dnia 18 czerwca 2020 r. w sprawie ustanowienia ram ułatwiających zrównoważone inwestycje, Dz. Urz. UE L 198 z 22.06.2020, s. 13.
7) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1060 z dnia 24 czerwca 2021 r. ustanawiające wspólne przepisy dotyczące funduszy europejskich, Dz. Urz. UE L 231 z 30.06.2021, s. 159.

2.1.2. Umowy międzynarodowe

1) Umowa między Rządem Rzeczypospolitej Polskiej i Rządem Republiki Federalnej Niemiec o żegludze śródlądowej, sporządzona w Warszawie dnia 8 listopada 1991 r.
2) Umowa między Rzecząpospolitą Polską a Republiką Federalną Niemiec o współpracy w dziedzinie gospodarki wodnej na wodach granicznych, sporządzona w Warszawie dnia 19 maja 1992 r.
3) Umowa w sprawie Międzynarodowej Komisji Ochrony Odry przed Zanieczyszczeniem, sporządzona we Wrocławiu dnia 11 kwietnia 1996 r.
4) Europejskie porozumienie w sprawie głównych śródlądowych dróg wodnych o znaczeniu międzynarodowym (AGN), sporządzone w Genewie dnia 19 stycznia 1996 r.
5) Regulamin radiokomunikacyjny Międzynarodowego Związku Telekomunikacyjnego (ITU Radio Regulations) w zakresie służb radiokomunikacyjnych wykorzystywanych dla żeglugi śródlądowej, radiokomunikacji ruchomej, stałej i satelitarnej.

2.1.3. Polskie przepisy prawne w randze ustawy

2.1.3.1. Zamówienia publiczne, umowy, finanse publiczne i realizacja inwestycji

1) Ustawa z dnia 11 września 2019 r. – Prawo zamówień publicznych, Dz.U. 2019 poz. 2019, tj. Dz.U. 2026 poz. 793.
2) Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny, tj. Dz.U. 2026 poz. 795.
3) Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych, tj. Dz.U. 2025 poz. 1483.

4) Ustawa z dnia 17 grudnia 2004 r. o odpowiedzialności za naruszenie dyscypliny finansów publicznych, tj. Dz.U. 2025 poz. 1484.
5) Ustawa z dnia 29 września 1994 r. o rachunkowości, tj. Dz.U. 2026 poz. 522.
6) Ustawa z dnia 11 marca 2004 r. o podatku od towarów i usług, tj. Dz.U. 2025 poz. 775.
7) Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej, tj. Dz.U. 2022 poz. 902.
8) Ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego, tj. Dz.U. 2023 poz. 1524.

2.1.3.2. Żegluga śródlądowa, RIS, gospodarka wodna i drogi wodne

1) Ustawa z dnia 21 grudnia 2000 r. o żegludze śródlądowej, Dz.U. 2001 Nr 5 poz. 43, tj. Dz.U. 2025 poz. 18.
2) Ustawa z dnia 20 lipca 2017 r. – Prawo wodne, Dz.U. 2017 poz. 1566, tj. Dz.U. 2025 poz. 960.
3) Ustawa z dnia 20 grudnia 1996 r. o portach i przystaniach morskich, tj. Dz.U. 2021 poz. 679.
4) Ustawa z dnia 28 października 2002 r. o Funduszu Żeglugi Śródlądowej i Funduszu Rezerwowym, tj. Dz.U. 2017 poz. 2095.
5) Ustawa z dnia 13 lipca 2023 r. o rewitalizacji rzeki Odry, Dz.U. 2023 poz. 1963.
6) Ustawa z dnia 18 sierpnia 2011 r. o bezpieczeństwie osób przebywających na obszarach wodnych, tj. Dz.U. 2023 poz. 714.
7) Ustawa z dnia 18 kwietnia 1985 r. o rybactwie śródlądowym, tj. Dz.U. 2022 poz. 883.
8) Ustawa z dnia 12 października 1990 r. o ochronie granicy państwowej, tj. Dz.U. 2025 poz. 184.

2.1.3.3. Budownictwo, planowanie przestrzenne, geodezja, drogi i przeszkody lotnicze

1) Ustawa z dnia 7 lipca 1994 r. – Prawo budowlane, Dz.U. 1994 Nr 89 poz. 414, tj. Dz.U. 2026 poz. 524.
2) Ustawa z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym, Dz.U. 2003 Nr 80 poz. 717, tj. Dz.U. 2026 poz. 538.
3) Ustawa z dnia 16 kwietnia 2004 r. o wyrobach budowlanych, Dz.U. 2004 Nr 92 poz. 881, tj. Dz.U. 2021 poz. 1213.
4) Ustawa z dnia 17 maja 1989 r. – Prawo geodezyjne i kartograficzne, Dz.U. 1989 Nr 30 poz. 163, tj. Dz.U. 2024 poz. 1151.
5) Ustawa z dnia 21 marca 1985 r. o drogach publicznych, Dz.U. 1985 Nr 14 poz. 60, tj. Dz.U. 2025 poz. 889.

6) Ustawa z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym, tj. Dz.U. 2024 poz. 1251.
7) Ustawa z dnia 3 lipca 2002 r. – Prawo lotnicze, Dz.U. 2002 Nr 130 poz. 1112, tj. Dz.U. 2025 poz. 1431.
8) Ustawa z dnia 23 lipca 2003 r. o ochronie zabytków i opiece nad zabytkami, tj. Dz.U. 2024 poz. 1292.
9) Ustawa z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze, tj. Dz.U. 2026 poz. 69.

2.1.3.4. Komunikacja elektroniczna, radiokomunikacja, cyberbezpieczeństwo, dane i dostępność cyfrowa

W zakresie projektowania, wykonania, dostarczenia, wdrożenia, integracji, utrzymania i eksploatacji systemów teleinformatycznych, usług cyfrowych, komunikacji elektronicznej, radiokomunikacji, cyberbezpieczeństwa, przetwarzania danych, interoperacyjności oraz dostępności cyfrowej zastosowanie mają w szczególności następujące akty prawa krajowego:

1) Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych, tj. Dz.U. 2023 poz. 1440, z późniejszymi zmianami — w zakresie obowiązku zapewnienia dostępności cyfrowej stron internetowych, aplikacji mobilnych, usług cyfrowych, deklaracji dostępności oraz wymagań dotyczących projektowania, wdrażania, utrzymania i aktualizacji rozwiązań cyfrowych podmiotu publicznego.
2) Ustawa z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami, tj. Dz.U. 2024 poz. 1411, z późniejszymi zmianami — w zakresie zapewniania dostępności osobom ze szczególnymi potrzebami, w tym dostępności informacyjno-komunikacyjnej, organizacyjnej i cyfrowej, w zakresie mającym zastosowanie do usług, dokumentacji, informacji, komunikacji i rozwiązań dostarczanych w ramach zamówienia.
3) Ustawa z dnia 26 kwietnia 2024 r. o zapewnianiu spełniania wymagań dostępności niektórych produktów i usług przez podmioty gospodarcze, Dz.U. 2024 poz. 731, z późniejszymi zmianami — w zakresie wymagań dostępności produktów i usług objętych zakresem ustawy, jeżeli dostarczane przez Generalnego Wykonawcę produkty, usługi, komponenty aplikacyjne, terminale, interfejsy, aplikacje albo usługi cyfrowe mieszczą się w jej zakresie zastosowania.
4) Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, tj. Dz.U. 2024 poz. 1557, z późniejszymi zmianami — w zakresie informatyzacji działalności podmiotów publicznych, interoperacyjności, wymiany informacji drogą elektroniczną, minimalnych wymagań dla systemów teleinformatycznych, rejestrów publicznych, usług elektronicznych oraz dokumentów elektronicznych.
5) Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych, tj. Dz.U. 2024 poz. 1045, z późniejszymi zmianami — w zakresie, w jakim rozwiązania dostarczane w ramach zamówienia będą wykorzystywać mechanizmy doręczeń elektronicznych, komunikacji elektronicznej, dokumentów elektronicznych albo integracji z usługami publicznymi.
6) Ustawa z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej, Dz.U. 2024 poz. 1221, z późniejszymi zmianami — w zakresie świadczenia usług komunikacji elektronicznej, infrastruktury telekomunikacyjnej, sieci telekomunikacyjnych, usług transmisji danych,

bezpieczeństwa komunikacji, obowiązków przedsiębiorców komunikacji elektronicznej oraz wymagań dotyczących sieci i usług komunikacji elektronicznej, jeżeli mają zastosowanie do przedmiotu zamówienia.

7) Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, tj. Dz.U. 2024 poz. 34, z późniejszymi zmianami — w zakresie, w jakim przepisy tej ustawy zachowują zastosowanie do pozwoleń radiowych, eksploatacji urządzeń radiowych, warunków wykorzystania częstotliwości, sieci telekomunikacyjnych albo infrastruktury telekomunikacyjnej w okresie przejściowym lub w zakresie nieobjętym przepisami Prawa komunikacji elektronicznej.

8) Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, tj. Dz.U. 2024 poz. 1077, z późniejszymi zmianami — w zakresie zarządzania ryzykiem, zapewniania cyberbezpieczeństwa, obsługi incydentów, monitorowania, dokumentowania, raportowania i utrzymywania bezpieczeństwa sieci i systemów informatycznych wykorzystywanych w systemie RIS.

9) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, tj. Dz.U. 2019 poz. 1781, z późniejszymi zmianami — w zakresie krajowych przepisów dotyczących ochrony danych osobowych, w powiązaniu z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679.

10) Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, tj. Dz.U. 2023 poz. 1206, z późniejszymi zmianami — w zakresie, w jakim rozwiązania, integracje albo usługi systemu RIS będą wykorzystywane przez podmioty lub w procesach, do których ma zastosowanie ta ustawa.

11) Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej, tj. Dz.U. 2022 poz. 902, z późniejszymi zmianami — w zakresie udostępniania informacji publicznej, publikacji danych, informacji i dokumentów, jeżeli dane albo usługi dostarczane w ramach systemu RIS będą wykorzystywane do realizacji obowiązków informacyjnych Zamawiającego.

12) Ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego, tj. Dz.U. 2023 poz. 1524, z późniejszymi zmianami — w zakresie zasad ponownego wykorzystywania informacji sektora publicznego, otwartych danych, udostępniania danych, metadanych, API, formatów danych i interoperacyjności danych, jeżeli dane systemu RIS będą udostępniane jako informacje sektora publicznego.

13) Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej, tj. Dz.U. 2024 poz. 422, z późniejszymi zmianami — w zakresie usług zaufania, identyfikacji elektronicznej, podpisów elektronicznych, pieczęci elektronicznych, walidacji, znaczników czasu, uwierzytelniania i dokumentów elektronicznych, jeżeli mechanizmy te będą wykorzystywane w rozwiązaniach systemu RIS.

14) Ustawa z dnia 21 lutego 2019 r. o elektronicznym fakturowaniu w zamówieniach publicznych, koncesjach na roboty budowlane lub usługi oraz partnerstwie publiczno-prywatnym, tj. Dz.U. 2020 poz. 1666, z późniejszymi zmianami — w zakresie, w jakim realizacja zamówienia, rozliczenia, komunikacja albo dokumentacja będą prowadzone z wykorzystaniem elektronicznego fakturowania lub powiązanych usług elektronicznych.

15) Ustawa z dnia 11 września 2019 r. – Prawo zamówień publicznych, tj. Dz.U. 2024 poz. 1320, z późniejszymi zmianami — w zakresie uwzględnienia dostępności dla osób z niepełnosprawnościami oraz projektowania z przeznaczeniem dla wszystkich użytkowników przy opisie przedmiotu zamówienia, a także w zakresie wymagań dotyczących środków komunikacji elektronicznej, dokumentowania i realizacji zamówienia publicznego.

2.1.3.5. Środowisko, odpady, BHP i ochrona przeciwpożarowa

1) Ustawa z dnia 27 kwietnia 2001 r. – Prawo ochrony środowiska, Dz.U. 2001 Nr 62 poz. 627, tj. Dz.U. 2025 poz. 647.
2) Ustawa z dnia 3 października 2008 r. o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz ocenach oddziaływania na środowisko, Dz.U. 2008 Nr 199 poz. 1227, tj. Dz.U. 2026 poz. 670.
3) Ustawa z dnia 16 kwietnia 2004 r. o ochronie przyrody, Dz.U. 2004 Nr 92 poz. 880, tj. Dz.U. 2026 poz. 13.
4) Ustawa z dnia 14 grudnia 2012 r. o odpadach, Dz.U. 2013 poz. 21, tj. Dz.U. 2023 poz. 1587.
5) Ustawa z dnia 11 września 2015 r. o zużytym sprzęcie elektrycznym i elektronicznym, Dz.U. 2015 poz. 1688, tj. Dz.U. 2024 poz. 573.
6) Ustawa z dnia 24 kwietnia 2009 r. o bateriach i akumulatorach, Dz.U. 2009 Nr 79 poz. 666, tj. Dz.U. 2025 poz. 809.
7) Ustawa z dnia 13 czerwca 2013 r. o gospodarce opakowaniami i odpadami opakowaniowymi, tj. Dz.U. 2026 poz. 619.
8) Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej, Dz.U. 1991 Nr 81 poz. 351, tj. Dz.U. 2025 poz. 188.
9) Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy, Dz.U. 1974 Nr 24 poz. 141, tj. Dz.U. 2025 poz. 277.

2.1.4. Polskie przepisy prawne w randze rozporządzenia

2.1.4.1. PFU, dokumentacja projektowa, projekt budowlany i warunki techniczne obiektów

1) Rozporządzenie Ministra Rozwoju i Technologii z dnia 20 grudnia 2021 r. w sprawie szczegółowego zakresu i formy dokumentacji projektowej, specyfikacji technicznych wykonania i odbioru robót budowlanych oraz programu funkcjonalno-użytkowego, Dz.U. 2021 poz. 2454.
2) Rozporządzenie Ministra Rozwoju z dnia 11 września 2020 r. w sprawie szczegółowego zakresu i formy projektu budowlanego, Dz.U. 2020 poz. 1609, tj. Dz.U. 2022 poz. 1679.

3) Rozporządzenie Ministra Infrastruktury z dnia 12 kwietnia 2002 r. w sprawie warunków technicznych, jakim muszą odpowiadać budynki i ich usytuowanie, Dz.U. 2002 Nr 75 poz. 690, tj. Dz.U. 2022 poz. 1225.
4) Rozporządzenie Ministra Cyfryzacji z dnia 26 maja 2023 r. w sprawie warunków technicznych, jakim muszą odpowiadać telekomunikacyjne obiekty budowlane i ich usytuowanie, Dz.U. 2023 poz. 1040.
5) Rozporządzenie Ministra Cyfryzacji z dnia 26 maja 2023 r. w sprawie warunków technicznych, jakim muszą odpowiadać kanały technologiczne, Dz.U. 2023 poz. 1039.
6) Rozporządzenie Ministra Infrastruktury z dnia 24 czerwca 2022 r. w sprawie przepisów techniczno-budowlanych dotyczących dróg publicznych, Dz.U. 2022 poz. 1518.
7) Rozporządzenie Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 25 kwietnia 2012 r. w sprawie ustalania geotechnicznych warunków posadawiania obiektów budowlanych, Dz.U. 2012 poz. 463.
8) Rozporządzenie Ministra Rozwoju z dnia 18 sierpnia 2020 r. w sprawie standardów technicznych wykonywania geodezyjnych pomiarów sytuacyjnych i wysokościowych oraz opracowywania i przekazywania wyników tych pomiarów do państwowego zasobu geodezyjnego i kartograficznego, Dz.U. 2022 poz. 1670.
9) Rozporządzenie Ministra Rozwoju i Technologii z dnia 15 grudnia 2022 r. w sprawie dziennika budowy oraz systemu Elektroniczny Dziennik Budowy, Dz.U. 2023 poz. 45.
10) Rozporządzenie Rady Ministrów z dnia 15 października 2012 r. w sprawie państwowego systemu odniesień przestrzennych, tj. Dz.U. 2024 poz. 342, z późniejszymi zmianami – w zakresie stosowania państwowego systemu odniesień przestrzennych, układów współrzędnych, układów wysokościowych, prac geodezyjnych, map do celów projektowych, inwentaryzacji powykonawczej, danych przestrzennych oraz pomiarów wodowskazowych wykonywanych na potrzeby systemu RIS.

2.1.4.2. RIS, żegluga śródlądowa i drogi wodne

1) Rozporządzenie Rady Ministrów z dnia 7 maja 2002 r. w sprawie klasyfikacji śródlądowych dróg wodnych, Dz.U. 2002 Nr 77 poz. 695, tj. Dz.U. 2022 poz. 1170.
2) Rozporządzenie Ministra Infrastruktury z dnia 28 kwietnia 2003 r. w sprawie przepisów żeglugowych na śródlądowych drogach wodnych, Dz.U. 2003 Nr 212 poz. 2072.
3) Rozporządzenie Ministra Infrastruktury z dnia 23 grudnia 2002 r. w sprawie pilotażu na śródlądowych drogach wodnych, Dz.U. 2003 Nr 5 poz. 53.
4) Rozporządzenie Ministra Infrastruktury z dnia 18 lutego 2010 r. w sprawie wykazu śródlądowych dróg wodnych państw członkowskich Unii Europejskiej, Dz.U. 2010 Nr 32 poz. 172.
5) Rozporządzenie Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 10 stycznia 2012 r. w sprawie określenia dyrektora urzędu żeglugi śródlądowej właściwego miejscowo do zarządzania usługami informacji rzecznej, Dz.U. 2012 poz. 58.

6) Rozporządzenie Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 8 stycznia 2013 r. w sprawie wykazu śródlądowych dróg wodnych, na których wprowadza się usługi informacji rzecznej, Dz.U. 2013 poz. 80.
7) Rozporządzenie Ministra Infrastruktury z dnia 14 maja 2026 r. w sprawie udostępniania danych niezbędnych do funkcjonowania systemu usług informacji rzecznej (RIS), Dz.U. 2026 poz. 674.
8) Rozporządzenie Ministra Gospodarki Morskiej i Żeglugi Śródlądowej z dnia 24 września 2018 r. w sprawie terytorialnego zakresu działania dyrektorów urzędów żeglugi śródlądowej i siedzib ich urzędów oraz siedzib i właściwości miejscowej delegatur tych urzędów, tj. Dz.U. 2021 poz. 675.

2.1.4.3. Radiokomunikacja, częstotliwości, urządzenia radiowe i pola elektromagnetyczne

1) Rozporządzenie Rady Ministrów z dnia 27 grudnia 2013 r. w sprawie Krajowej Tablicy Przeznaczeń Częstotliwości, tj. Dz.U. 2023 poz. 2518, zmienione rozporządzeniem Rady Ministrów z dnia 15 lipca 2024 r., Dz.U. 2024 poz. 1141.
2) Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie pozwoleń dla służby radiokomunikacyjnej morskiej i żeglugi śródlądowej, Dz.U. 2015 poz. 10, w zakresie zachowanych lub przejściowo stosowanych decyzji i pozwoleń wydanych na jego podstawie.
3) Rozporządzenie Ministra Zdrowia z dnia 17 grudnia 2019 r. w sprawie dopuszczalnych poziomów pól elektromagnetycznych w środowisku, Dz.U. 2019 poz. 2448.
4) Rozporządzenie Ministra Klimatu z dnia 17 lutego 2020 r. w sprawie sposobów sprawdzania dotrzymania dopuszczalnych poziomów pól elektromagnetycznych w środowisku, Dz.U. 2020 poz. 258, tj. Dz.U. 2022 poz. 2630.
5) Rozporządzenie Ministra Środowiska z dnia 2 lipca 2010 r. w sprawie zgłoszenia instalacji wytwarzających pola elektromagnetyczne, Dz.U. 2010 Nr 130 poz. 879.
6) Rozporządzenie Ministra Środowiska z dnia 2 lipca 2010 r. w sprawie rodzajów instalacji, których eksploatacja wymaga zgłoszenia, Dz.U. 2010 Nr 130 poz. 880, tj. Dz.U. 2019 poz. 1510.
7) Obwieszczenie Ministra Cyfryzacji z dnia 17 maja 2026 r. w sprawie wykazu norm zharmonizowanych na potrzeby zgodności urządzeń radiowych z wymaganiami zasadniczymi, Dz.U. 2026 poz. 671.

2.1.4.4. Ochrona środowiska, odpady, oceny oddziaływania i gospodarka wodna

1) Rozporządzenie Rady Ministrów z dnia 10 września 2019 r. w sprawie przedsięwzięć mogących znacząco oddziaływać na środowisko, Dz.U. 2019 poz. 1839.

2) Rozporządzenie Ministra Klimatu i Środowiska z dnia 17 grudnia 2021 r. w sprawie wymaganych zakresów planów gospodarowania wodami na obszarach dorzeczy, Dz.U. 2021 poz. 2441.
3) Rozporządzenie Ministra Infrastruktury z dnia 16 listopada 2022 r. w sprawie Planu gospodarowania wodami na obszarze dorzecza Odry, Dz.U. 2023 poz. 335.
4) Rozporządzenie Ministra Infrastruktury z dnia 26 października 2022 r. w sprawie przyjęcia Planu zarządzania ryzykiem powodziowym dla obszaru dorzecza Odry, Dz.U. 2022 poz. 2714.
5) Rozporządzenie Ministra Klimatu z dnia 2 stycznia 2020 r. w sprawie katalogu odpadów, Dz.U. 2020 poz. 10.
6) Rozporządzenie Ministra Klimatu z dnia 11 września 2020 r. w sprawie szczegółowych wymagań dla magazynowania odpadów, Dz.U. 2020 poz. 1742.
7) Rozporządzenie Ministra Klimatu i Środowiska z dnia 7 września 2021 r. w sprawie wymagań dla prowadzenia procesu przetwarzania odpadów, Dz.U. 2021 poz. 1642.

2.1.4.5. BHP, ochrona przeciwpożarowa, organizacja robót i utrzymanie ruchu

1) Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 26 września 1997 r. w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy, Dz.U. 1997 Nr 129 poz. 844, tj. Dz.U. 2003 Nr 169 poz. 1650.
2) Rozporządzenie Ministra Infrastruktury z dnia 6 lutego 2003 r. w sprawie bezpieczeństwa i higieny pracy podczas wykonywania robót budowlanych, Dz.U. 2003 Nr 47 poz. 401.
3) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 7 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów, tj. Dz.U. 2023 poz. 822 z późniejszymi zmianami.
4) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 24 lipca 2009 r. w sprawie przeciwpożarowego zaopatrzenia w wodę oraz dróg pożarowych, Dz.U. 2009 Nr 124 poz. 1030.
5) Rozporządzenie Ministra Infrastruktury z dnia 23 września 2003 r. w sprawie szczegółowych warunków zarządzania ruchem na drogach oraz wykonywania nadzoru nad tym zarządzaniem, tj. Dz.U. 2017 poz. 784.
6) Rozporządzenie Ministrów Infrastruktury oraz Spraw Wewnętrznych i Administracji z dnia 31 lipca 2002 r. w sprawie znaków i sygnałów drogowych, tj. Dz.U. 2019 poz. 2310 z późniejszymi zmianami.
7) Rozporządzenie Ministra Infrastruktury z dnia 3 lipca 2003 r. w sprawie szczegółowych warunków technicznych dla znaków i sygnałów drogowych oraz urządzeń bezpieczeństwa ruchu drogowego i warunków ich umieszczania na drogach, tj. Dz.U. 2019 poz. 2311 z późniejszymi zmianami.

2.1.4.6. Krajowe Ramy Interoperacyjności i systemy teleinformatyczne administracji publicznej

1) Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. 2024 poz. 773.
2) Rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych, tj. Dz.U. 2018 poz. 180.
3) Rozporządzenie Ministra Cyfryzacji z dnia 12 sierpnia 2021 r. w sprawie profilu zaufanego i podpisu zaufanego, Dz.U. 2021 poz. 1076.

2.1.4.7. Przepisy prawa miejscowego i akty właściwych organów dla Odrzańskiej Drogi Wodnej

1) Zarządzenie nr 1/2021 Dyrektora Urzędu Żeglugi Śródlądowej we Wrocławiu z dnia 26 maja 2021 r. w sprawie szczegółowych warunków bezpieczeństwa ruchu i postoju statków; publikacja w dziennikach urzędowych właściwych województw, w szczególności: Dz. Urz. Woj. Dolnośląskiego z 26.05.2021 r. poz. 2550, Dz. Urz. Woj. Opolskiego z 26.05.2021 r. poz. 1385, Dz. Urz. Woj. Lubuskiego z 26.05.2021 r. poz. 1173, Dz. Urz. Woj. Śląskiego z 26.05.2021 r. poz. 3630.
2) Zarządzenie nr 1/2022 Dyrektora Urzędu Żeglugi Śródlądowej w Szczecinie z dnia 10 marca 2022 r. w sprawie uprawiania żeglugi na wodach granicznych rzek Odry, Odry Zachodniej i Nysy Łużyckiej; Dz. Urz. Woj. Zachodniopomorskiego z 11.03.2022 r. poz. 1124.
3) Obowiązujące zarządzenia, komunikaty nawigacyjne i czasowe ograniczenia administracji drogi wodnej oraz dyrektorów urzędów żeglugi śródlądowej właściwych dla lokalizacji robót i instalacji terenowych.
4) Obowiązujące akty prawa miejscowego jednostek samorządu terytorialnego w zakresie miejscowych planów zagospodarowania przestrzennego, ochrony konserwatorskiej, organizacji ruchu, dostępu do pasa drogowego, ochrony środowiska i zasad prowadzenia robót w przestrzeni publicznej, właściwe dla poszczególnych lokalizacji systemu RIS.

2.1.5. Normy i standardy techniczne

2.1.5.1. RIS, Inland ECDIS, Inland AIS, ERI, NtS i dane referencyjne

1) CESNI ES-RIS Edition 2025/1 – European Standard for River Information Services, obejmujący w szczególności Inland ECDIS, Vessel Tracking and Tracing/Inland AIS, Notices to Skippers oraz Electronic Ship Reporting.
2) CESNI ES-TRIN Edition 2025/1 – European Standard laying down Technical Requirements for Inland Navigation vessels, w zakresie powiązanym z RIS, AIS, urządzeniami pokładowymi i wymianą danych.
3) UNECE Resolution No. 48 – Recommendation on Electronic Chart Display and Information System for Inland Navigation (Inland ECDIS).
4) UNECE Resolution No. 57 – Guidelines and Recommendations for River Information Services.
5) UNECE Resolution No. 58 – Guidelines and Criteria for Vessel Traffic Services on Inland Waterways.
6) UNECE Resolution No. 63 – International Standard for Tracking and Tracing on Inland Waterways.
7) UNECE Resolution No. 79 – International Standard for Electronic Ship Reporting in Inland Navigation.
8) UNECE Resolution No. 80 – International Standard for Notices to Skippers and Electronic Reporting in Inland Navigation.
9) IHO S-57 – IHO Transfer Standard for Digital Hydrographic Data, wraz ze specyfikacjami produktowymi Inland ENC stosowanymi w RIS.
10) IHO S-52 – Specifications for Chart Content and Display Aspects of ECDIS.
11) IHO S-63 – IHO Data Protection Scheme.
12) IHO S-100 – Universal Hydrographic Data Model, w zakresie przygotowania do rozwiązań nowej generacji.
13) ERI XSD/XML, RIS Index, ERDMS, ISRS Location Codes, ENC/IENC Encoding Guides oraz aktualne słowniki i kody referencyjne publikowane dla RIS.

2.1.5.2. Radiokomunikacja VHF, AIS, DGNSS, propagacja i urządzenia radiowe

1) ITU Radio Regulations – postanowienia dotyczące przydziału częstotliwości, identyfikacji stacji, kanałów i procedur radiokomunikacyjnych.
2) ITU-R M.1371 – Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band.
3) ITU-R M.1084 – Interim solutions for improved efficiency in the use of the band 156–174 MHz by stations in the maritime mobile service.

4) ITU-R M.493 – Digital selective-calling system for use in the maritime mobile service, w zakresie urządzeń i funkcji wykorzystujących DSC.
5) IEC 61993-2 – Maritime navigation and radiocommunication equipment and systems – Automatic identification systems (AIS) – Class A shipborne equipment.
6) IEC 62320-1 – Maritime navigation and radiocommunication equipment and systems – AIS base stations.
7) IEC 62320-2 – AIS AtoN stations.
8) IEC 62320-3 – AIS repeater stations.
9) IEC 61108 – Global navigation satellite systems, w zakresie urządzeń GNSS/DGNSS.
10) RTCM Standard 10403.x – Differential GNSS services, w zakresie transmisji poprawek różnicowych.
11) ETSI EN 301 178 – Portable VHF radiotelephone equipment for the maritime mobile service operating in the VHF bands.
12) ETSI EN 301 843 – Electromagnetic compatibility standard for marine radio equipment and services.
13) ETSI EN 302 217 – Fixed Radio Systems; characteristics and requirements for point-to-point equipment and antennas.
14) ETSI EN 301 893 i ETSI EN 302 502 – urządzenia szerokopasmowe i systemy transmisji w pasmach RLAN, w zakresie zastosowanych urządzeń radiowych nielicencjonowanych.
15) ETSI EN 303 413 – Satellite Earth Stations and Systems; Global Navigation Satellite System receivers; radio equipment operating in the 1 164 MHz to 1 300 MHz and 1 559 MHz to 1 610 MHz frequency bands.

2.1.5.3. CCTV/VSS, transmisja i zapis obrazu

1) PN-EN IEC 62676 – Systemy dozoru wizyjnego stosowane w zabezpieczeniach, wszystkie właściwe części normy.
2) PN-EN IEC 62676-1-1 – Systemy dozoru wizyjnego stosowane w zabezpieczeniach – Wymagania systemowe.
3) PN-EN IEC 62676-1-2 – Wymagania dotyczące transmisji wizyjnej.
4) PN-EN IEC 62676-2-31 – Protokoły transmisji wideo IP – Profilowanie i interfejsy.
5) PN-EN IEC 62676-2-32 – Protokoły transmisji wideo IP – Interoperacyjność oparta na usługach sieciowych.
6) PN-EN IEC 62676-4 – Wytyczne stosowania systemów dozoru wizyjnego.
7) ONVIF Profile S, Profile T, Profile G i Profile M – interoperacyjność kamer IP, rejestratorów, strumieni wideo, metadanych i zdarzeń.
8) ITU-T H.264 / ISO/IEC 14496-10 oraz ITU-T H.265 / ISO/IEC 23008-2 – kompresja obrazu wideo.
9) RFC 3550 – RTP: A Transport Protocol for Real-Time Applications.

10) RFC 7826 – Real-Time Streaming Protocol Version 2.0.
11) PN-EN IEC 60529 – Stopnie ochrony zapewnianej przez obudowy (kod IP).
12) PN-EN IEC 62262 – Stopnie ochrony przed zewnętrznymi uderzeniami mechanicznymi (kod IK).

2.1.5.4. Sieci IP, transmisja danych, synchronizacja czasu i zarządzanie

1) ISO/IEC/IEEE 8802-3 – Ethernet.
2) IEEE 802.1Q – VLANs and Bridged Networks.
3) IEEE 802.1X – Port-Based Network Access Control.
4) IEEE 802.1AX – Link Aggregation.
5) RFC 791 – Internet Protocol IPv4.
6) RFC 8200 – Internet Protocol Version 6.
7) RFC 4301 – Security Architecture for the Internet Protocol.
8) RFC 7296 – Internet Key Exchange Protocol Version 2 (IKEv2).
9) RFC 8446 – The Transport Layer Security (TLS) Protocol Version 1.3.
10) RFC 5905 – Network Time Protocol Version 4.
11) IEEE 1588 – Precision Time Protocol, w zakresie wymaganej synchronizacji czasu urządzeń.
12) RFC 5424 – The Syslog Protocol.
13) RFC 3411, RFC 3414 i RFC 3415 – SNMPv3 architecture, security and access control.
14) RFC 6241 – Network Configuration Protocol (NETCONF).
15) RFC 7950 – The YANG 1.1 Data Modeling Language.
16) 3GPP Technical Specifications dla LTE/5G NR, w zakresie transmisji z wykorzystaniem publicznych sieci komórkowych i prywatnych APN.

2.1.5.5. Cyberbezpieczeństwo, bezpieczeństwo informacji i ciągłość działania

1) PN-EN ISO/IEC 27001 – Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Systemy zarządzania bezpieczeństwem informacji – Wymagania.
2) PN-EN ISO/IEC 27002 – Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Zabezpieczenia informacji.
3) PN-EN ISO/IEC 27005 – Zarządzanie ryzykiem w bezpieczeństwie informacji.
4) ISO/IEC 27017 – Code of practice for information security controls based on ISO/IEC 27002 for cloud services.
5) ISO/IEC 27018 – Protection of personally identifiable information in public clouds.

6) ISO/IEC 27701 – Privacy Information Management.
7) ISO/IEC 27035 – Information security incident management.
8) PN-EN ISO 22301 – Security and resilience – Business continuity management systems – Requirements.
9) PN-ISO 31000 – Zarządzanie ryzykiem – Wytyczne.
10) IEC 62443 – Industrial communication networks – Network and system security, w zakresie segmentacji, ochrony urządzeń i sieci OT/IoT.
11) NIST Cybersecurity Framework 2.0.
12) CIS Critical Security Controls v8.
13) OWASP Web Security Testing Guide, OWASP ASVS, OWASP Top 10 oraz OWASP API Security Top 10, w zakresie usług i interfejsów aplikacyjnych.
14) BSI IT-Grundschutz, w zakresie stosowania wzorców zabezpieczeń infrastruktury teleinformatycznej.

2.1.5.6. Okablowanie, serwerownie, zasilanie, EMC i urządzenia elektryczne

1) PN-EN 50173 – Technika informatyczna – Systemy okablowania strukturalnego.
2) PN-EN 50174 – Technika informatyczna – Instalacja okablowania.
3) PN-EN 50310 – Stosowanie połączeń wyrównawczych i uziemiających w budynkach z zainstalowanymi urządzeniami techniki informatycznej.
4) ISO/IEC 11801 – Information technology – Generic cabling for customer premises.
5) PN-EN 50600 – Technika informatyczna – Wyposażenie i infrastruktura centrów przetwarzania danych.
6) TIA-942 – Telecommunications Infrastructure Standard for Data Centers.
7) PN-HD 60364 – Instalacje elektryczne niskiego napięcia, wszystkie właściwe części normy.
8) PN-EN IEC 61439 – Rozdzielnice i sterownice niskonapięciowe.
9) PN-EN IEC 62040 – Systemy bezprzerwowego zasilania UPS, wszystkie właściwe części normy.
10) PN-EN IEC 61643 – Urządzenia ograniczające przepięcia niskonapięciowe.
11) PN-EN IEC 62368-1 – Urządzenia techniki fonicznej/wizyjnej, informatycznej i telekomunikacyjnej – Wymagania bezpieczeństwa.
12) PN-EN 55032 – Kompatybilność elektromagnetyczna urządzeń multimedialnych – Wymagania dotyczące emisji.
13) PN-EN 55035 – Kompatybilność elektromagnetyczna urządzeń multimedialnych – Wymagania dotyczące odporności.

14) PN-EN IEC 61000 – Kompatybilność elektromagnetyczna, wszystkie właściwe części normy.
15) PN-EN IEC 62305 – Ochrona odgromowa, wszystkie właściwe części normy.
16) PN-EN IEC 60529 – Stopnie ochrony zapewnianej przez obudowy (kod IP).
17) PN-EN IEC 62262 – Stopnie ochrony przed zewnętrznymi uderzeniami mechanicznymi (kod IK).

2.1.5.7. Konstrukcje budowlane, wieże, maszty, wsporniki, fundamenty i zabezpieczenia antykorozyjne

1) PN-EN 1990 – Eurokod: Podstawy projektowania konstrukcji.
2) PN-EN 1991 – Eurokod 1: Oddziaływania na konstrukcje, w szczególności obciążenie wiatrem, śniegiem, temperaturą, oblodzeniem i oddziaływania wyjątkowe.
3) PN-EN 1992 – Eurokod 2: Projektowanie konstrukcji z betonu.
4) PN-EN 1993 – Eurokod 3: Projektowanie konstrukcji stalowych.
5) PN-EN 1993-3-1 – Eurokod 3: Wieże, maszty i kominy – Wieże i maszty.
6) PN-EN 1997 – Eurokod 7: Projektowanie geotechniczne.
7) PN-EN 1998 – Eurokod 8: Projektowanie konstrukcji poddanych oddziaływaniom sejsmicznym, w zakresie właściwym dla lokalizacji i kategorii obiektu.
8) PN-EN 1090-1 – Wykonanie konstrukcji stalowych i aluminiowych – Zasady oceny zgodności elementów konstrukcyjnych.
9) PN-EN 1090-2 – Wykonanie konstrukcji stalowych i aluminiowych – Wymagania techniczne dotyczące konstrukcji stalowych.
10) PN-EN ISO 1461 – Powłoki cynkowe nanoszone na wyroby stalowe i żeliwne metodą zanurzeniową.
11) PN-EN ISO 12944 – Farby i lakiery – Ochrona przed korozją konstrukcji stalowych za pomocą ochronnych systemów malarskich.
12) PN-EN ISO 14713 – Powłoki cynkowe – Wytyczne i zalecenia dotyczące ochrony przed korozją konstrukcji ze stali i żeliwa.
13) PN-EN ISO 3834 – Wymagania jakości dotyczące spawania materiałów metalowych.
14) PN-EN ISO 9606 – Egzamin kwalifikacyjny spawaczy.
15) PN-EN ISO 5817 – Spawanie – Złącza spawane ze stali, niklu, tytanu i ich stopów – Poziomy jakości według niezgodności spawalniczych.

2.1.5.8. Jakość, zarządzanie projektem, testy, niezawodność i utrzymanie

1) PN-EN ISO 9001 – Systemy zarządzania jakością – Wymagania.

2) PN-EN ISO 14001 – Systemy zarządzania środowiskowego – Wymagania i wytyczne stosowania.
3) PN-ISO 45001 – Systemy zarządzania bezpieczeństwem i higieną pracy – Wymagania i wytyczne stosowania.
4) PN-ISO 10005 – Zarządzanie jakością – Wytyczne dotyczące planów jakości.
5) ISO 21502 – Project, programme and portfolio management – Guidance on project management.
6) ISO/IEC/IEEE 12207 – Systems and software engineering – Software life cycle processes.
7) ISO/IEC/IEEE 15288 – Systems and software engineering – System life cycle processes.
8) ISO/IEC 25010 – Systems and software quality models.
9) ISO/IEC/IEEE 29119 – Software and systems engineering – Software testing.
10) IEC 60068 – Environmental testing, w zakresie badań środowiskowych urządzeń terenowych.
11) IEC 60529 oraz IEC 62262 – badania stopnia ochrony obudów IP/IK urządzeń terenowych.
12) World Meteorological Organization (WMO), Guide to Instruments and Methods of Observation, WMO-No. 8, Volumes I–V, aktualne wydanie, Geneva, Switzerland, wraz z późniejszymi zmianami i aktualizacjami - w zakresie właściwym dla doboru, lokalizacji, instalacji, eksploatacji, kontroli, dokumentowania, testowania i weryfikacji urządzeń oraz metod pomiarów meteorologicznych stosowanych dla sensorów meteorologicznych systemu RIS.

2.1.5.9. Dostępność cyfrowa, WCAG i dostępność produktów oraz usług ICT

1) EN 301 549 V3.2.1 (2021-03), Accessibility requirements for ICT products and services, albo aktualna wersja normy zharmonizowanej wskazana w Dzienniku Urzędowym UE dla właściwego aktu prawnego;
2) Web Content Accessibility Guidelines (WCAG) 2.1, poziom AA — jako minimalny poziom wymagany przepisami dla stron internetowych i aplikacji mobilnych podmiotów publicznych;
3) Web Content Accessibility Guidelines (WCAG) 2.2, poziom AA — jako standard rekomendowany dla nowo projektowanych lub modernizowanych rozwiązań, o ile nie pozostaje w sprzeczności z obowiązującym standardem zharmonizowanym;
4) WAI-ARIA Authoring Practices oraz właściwe wytyczne W3C/WAI — w zakresie komponentów interfejsu użytkownika, obsługi technologii wspomagających i aplikacji webowych.

2.1.6. Pozostałe dokumenty programowe, wytyczne i dokumenty odniesienia

2.1.6.1. Dokumenty programowe i finansowanie

1) Program Fundusze Europejskie na Infrastrukturę, Klimat, Środowisko 2021–2027 (FEnIKS).
2) Szczegółowy Opis Priorytetów Programu Fundusze Europejskie na Infrastrukturę, Klimat, Środowisko 2021–2027.
3) Umowa o dofinansowanie projektu „Rozbudowa systemu RIS na Odrzańskiej Drodze Wodnej”, FENX.04.04-IP.02-0001/24.
4) Wytyczne dotyczące kwalifikowalności wydatków na lata 2021–2027.
5) Wytyczne dotyczące informacji i promocji Funduszy Europejskich na lata 2021–2027.
6) Wytyczne dotyczące realizacji zasad równościowych w ramach funduszy unijnych na lata 2021–2027.
7) Wytyczne dotyczące kontroli realizacji programów polityki spójności na lata 2021–2027.
8) Wytyczne Komisji Europejskiej dotyczące zasady „nie czyń poważnych szkód” (DNSH) oraz dokumenty programowe FEnIKS w zakresie DNSH i odporności klimatycznej.
9) Technical guidance on the climate proofing of infrastructure in the period 2021–2027, Komisja Europejska, 2021/C 373/01.
10) JASPERS Guidance Note: The Basics of Climate Change Adaptation, Vulnerability and Risk Assessment, w zakresie infrastruktury współfinansowanej ze środków UE.

2.1.6.2. Dokumenty strategiczne i branżowe dla żeglugi śródlądowej, transportu i gospodarki wodnej

1) Krajowy Program Żeglugowy do roku 2030.
2) Strategia Zrównoważonego Rozwoju Transportu do 2030 roku.
3) Strategia na rzecz Odpowiedzialnego Rozwoju do roku 2020 z perspektywą do 2030 roku.
4) Program przeciwdziałania niedoborowi wody.
5) Plan gospodarowania wodami na obszarze dorzecza Odry.
6) Plan zarządzania ryzykiem powodziowym dla obszaru dorzecza Odry.
7) Mapy zagrożenia powodziowego i mapy ryzyka powodziowego dla obszarów objętych projektem.
8) Dokumenty planistyczne, studialne i operacyjne Państwowego Gospodarstwa Wodnego Wody Polskie właściwe dla Odrzańskiej Drogi Wodnej.
9) Komunikaty nawigacyjne, informatory i mapy publikowane przez administrację drogi wodnej oraz właściwe urzędy żeglugi śródlądowej.

2.1.6.3. Dokumenty odniesienia dla systemu RIS i komponentów teleinformatycznych

1) RIS Index, European Reference Data Management System (ERDMS), RIS COMEX Reference Data oraz właściwe słowniki referencyjne RIS.
2) Wytyczne, dokumentacja techniczna i interoperacyjna CESNI, UNECE, IHO, ITU, ETSI, IEC, ISO, IEEE, IETF i ONVIF właściwe dla zastosowanych technologii.
3) Aktualne decyzje, pozwolenia radiowe, warunki wykorzystania częstotliwości i plany zagospodarowania częstotliwości właściwe dla urządzeń radiowych VHF, AIS, DGNSS, radiolinii i urządzeń transmisji bezprzewodowej.
4) Obowiązujące dokumenty bezpieczeństwa, polityki, procedury i instrukcje eksploatacyjne Zamawiającego dotyczące systemu RIS, w zakresie udostępnionym na potrzeby realizacji przedmiotu zamówienia.
5) Dokumentacja powykonawcza i eksploatacyjna istniejącego systemu RIS Dolnej Odry w zakresie wymaganym dla zachowania kompatybilności, ciągłości działania i integracji z nowymi komponentami.
6) Plan systemu monitoringu wizyjnego (CCTV), Plan łączności radiowej VHF/AIS oraz Plan połączeń transmisyjnych opracowane dla projektu „Rozbudowa systemu RIS na Odrzańskiej Drodze Wodnej”.
7) Studium wykonalności dla projektu „Rozbudowa systemu RIS na Odrzańskiej Drodze Wodnej”.

2.2. Informacje i dokumenty niezbędne do zaprojektowania robót budowlanych oraz wykonania zamierzenia inwestycyjnego

2.2.1. Postanowienia ogólne

1) Przedmiot Zamówienia jest realizowany w formule „zaprojektuj i zbuduj”. Generalny Wykonawca odpowiada za pozyskanie, weryfikację, aktualizację, opracowanie i uzgodnienie wszystkich informacji, materiałów, dokumentów, decyzji, opinii, ekspertyz, pozwoleń, zgód, warunków technicznych i warunków realizacyjnych niezbędnych do prawidłowego zaprojektowania, wykonania, uruchomienia, odbioru i przekazania do eksploatacji robót oraz infrastruktury objętej Zamówieniem.
2) Generalny Wykonawca musi ująć w cenie oferty koszt wszystkich prac, czynności projektowych, badań, pomiarów, analiz, uzgodnień, ekspertyz, opinii, map, opracowań geodezyjnych, geotechnicznych, środowiskowych, wodnoprawnych, konserwatorskich, konstrukcyjnych, branżowych, radiowych, formalnoprawnych i administracyjnych, a także koszt uzyskania wszystkich wymaganych decyzji administracyjnych, pozwoleń, zgód, warunków technicznych i warunków realizacyjnych.
3) Brak wyszczególnienia określonego dokumentu, decyzji, zgody, pozwolenia, opinii, ekspertyzy lub uzgodnienia w niniejszym PFU nie zwalnia Generalnego Wykonawcy

z obowiązku jego uzyskania, jeżeli obowiązek ten wynika z przepisów prawa, wymagań właściwych organów, wymagań zarządców terenów lub obiektów, warunków technicznych, zasad wiedzy technicznej albo konieczności prawidłowego zaprojektowania i wykonania Przedmiotu Zamówienia.

4) Dokumenty, dane i informacje przekazane przez Zamawiającego mają charakter materiałów wyjściowych. Generalny Wykonawca musi zweryfikować ich aktualność, kompletność, przydatność projektową i zgodność ze stanem faktycznym w terenie. W przypadku stwierdzenia rozbieżności Generalny Wykonawca wykona dodatkowe rozpoznanie, uzyska aktualne dane i opracuje rozwiązania projektowe zgodne z aktualnym stanem prawnym, technicznym i terenowym.

5) Generalny Wykonawca działa w imieniu Zamawiającego w zakresie wynikającym z udzielonych pełnomocnictw. Uzyskanie pełnomocnictwa nie ogranicza odpowiedzialności Generalnego Wykonawcy za terminowe i kompletne przeprowadzenie procedur administracyjnych i uzgodnieniowych.

6) Generalny Wykonawca musi zapewnić, że dokumentacja projektowa będzie kompletna z punktu widzenia celu, któremu ma służyć, tj. umożliwi uzyskanie wymaganych decyzji i pozwoleń, wykonanie robót, dokonanie odbiorów, uzyskanie dopuszczeń do użytkowania oraz bezpieczną eksploatację infrastruktury RIS.

2.2.2. Zakres dokumentacji projektowej wymaganej w ramach Zamówienia

1) Generalny Wykonawca opracuje dokumentację projektową dla wszystkich elementów infrastruktury objętych Zamówieniem, w szczególności dla:
   a) nowych wież antenowych, masztów, konstrukcji wsporczych i instalacji antenowych systemów VHF/AIS;
   b) rozbiórek istniejących wież, masztów, konstrukcji wsporczych, szaf, instalacji i elementów kolidujących z projektowanym zakresem;
   c) montażu kamer, wodowskazów, czujników hydrologicznych, czujników meteorologicznych, szaf teletechnicznych, urządzeń transmisyjnych i zasilających na istniejących obiektach budowlanych, obiektach mostowych, obiektach hydrotechnicznych i terenach zarządców zewnętrznych;
   d) przyłączy elektroenergetycznych, wewnętrznych linii zasilających, zasilania gwarantowanego, uziemienia, ochrony odgromowej i ochrony przepięciowej;
   e) tras kablowych, kanalizacji kablowej, przepustów, przewiertów, przejść przez obiekty budowlane, przejść przez pasy drogowe, tereny kolejowe, tereny wodne i obiekty hydrotechniczne;
   f) elementów systemu transmisji danych, w tym urządzeń aktywnych, anten, torów radiowych, szaf, punktów styku i tras kablowych;
   g) robót adaptacyjnych, odtworzeniowych, zabezpieczających i kolizyjnych;

h) oznakowania przeszkodowego, jeżeli będzie wymagane ze względu na wysokość, lokalizację lub sąsiedztwo lądowisk, lotnisk albo powierzchni ograniczających przeszkody.

2) Dokumentacja projektowa musi obejmować co najmniej:

a) analizę uwarunkowań planistycznych i formalnoprawnych;

b) projekt zagospodarowania działki lub terenu;

c) projekt architektoniczno-budowlany, jeżeli jest wymagany;

d) projekt techniczny;

e) projekty wykonawcze w zakresie niezbędnym do jednoznacznego wykonania robót;

f) projekty branżowe, w szczególności konstrukcyjne, elektryczne, teletechniczne, telekomunikacyjne, odgromowe, uziemiające, drogowe, organizacji ruchu, sanitarne oraz inne wynikające z kolizji lub uwarunkowań lokalizacyjnych;

g) specyfikacje techniczne wykonania i odbioru robót;

h) informację BIOZ oraz plan BIOZ, jeżeli jest wymagany;

i) dokumentację uzgodnieniową dla zarządców terenów, zarządców obiektów, gestorów sieci i właściwych organów;

j) dokumentację powykonawczą i geodezyjną inwentaryzację powykonawczą.

3) W przypadku zastosowania projektu typowego wieży lub masztu Generalny Wykonawca musi wykonać jego pełną adaptację do warunków konkretnej działki, obejmującą w szczególności warunki gruntowo-wodne, oddziaływanie wiatru i oblodzenia, kategorię geotechniczną, sposób posadowienia, strefę przemarzania, uwarunkowania hydrologiczne, warunki dostępu serwisowego, kolizje z infrastrukturą istniejącą, lokalne wymagania zarządcy terenu oraz wymagania eksploatacyjne systemu RIS.

2.2.3. Mapy, materiały geodezyjne i obsługa geodezyjna

1) Generalny Wykonawca musi pozyskać aktualne materiały z państwowego zasobu geodezyjnego i kartograficznego oraz opracować mapy do celów projektowych w zakresie niezbędnym do zaprojektowania i wykonania Przedmiotu Zamówienia.

2) Zakres map do celów projektowych musi obejmować teren lokalizacji zasadniczej, teren niezbędny do wykonania przyłączy, tras kablowych, dróg dojazdowych, dojść serwisowych, placów montażowych, stref oddziaływania robót oraz obszary kolizji z istniejącym uzbrojeniem terenu.

3) Generalny Wykonawca wykona pomiary geodezyjne, inwentaryzację istniejącego uzbrojenia terenu, wytyczenie projektowanych obiektów, obsługę geodezyjną robót oraz geodezyjną inwentaryzację powykonawczą wraz z przekazaniem dokumentacji do właściwego ośrodka dokumentacji geodezyjnej i kartograficznej.

4) W przypadku obiektów mostowych, hydrotechnicznych, kolejowych i drogowych Generalny Wykonawca musi pozyskać również dostępne materiały archiwalne, dokumentację zarządcy obiektu, przekroje, rzuty, schematy instalacyjne i dane

konstrukcyjne w zakresie niezbędnym do bezpiecznego zaprojektowania mocowań, tras kablowych i urządzeń.

2.2.4. Operat Techniczny z pomiarów wodowskazów

1) Generalny Wykonawca zobowiązany jest opracować, uzgodnić z Zamawiającym i przekazać do akceptacji Operat Techniczny z pomiarów wodowskazów na obszarze działania rozbudowy systemu RIS na Odrzańskiej Drodze Wodnej. Operat Techniczny stanowi dokument niezbędny do zaprojektowania, wykonania, kalibracji, odbioru i późniejszej eksploatacji czujników hydrologicznych pełniących funkcję wodowskazów systemu RIS.
2) Operat Techniczny musi zostać opracowany dla wszystkich lokalizacji wodowskazowych objętych zakresem zamówienia, w których będą instalowane, uruchamiane, kalibrowane albo integrowane czujniki hydrologiczne. Dokument musi umożliwiać jednoznaczne powiązanie każdego punktu pomiarowego z właściwą osnową geodezyjną, układem współrzędnych, układem wysokościowym, zerem wodowskazu, miejscem montażu czujnika, rzędną odniesienia oraz wartościami wykorzystywanymi do kalibracji i weryfikacji poprawności wskazań.
3) Operat Techniczny musi obejmować co najmniej:
    a) sprawozdanie techniczne z wykonanych prac geodezyjnych i pomiarowych;
    b) określenie celu, zakresu rzeczowego i terytorialnego wykonanych prac;
    c) wykaz lokalizacji wodowskazowych objętych opracowaniem;
    d) wykaz wykorzystanych reperów i punktów podstawowej albo szczegółowej osnowy geodezyjnej;
    e) opisy topograficzne punktów osnowy i punktów odniesienia wykorzystanych do pomiaru;
    f) opis metody pomiaru oraz sprzętu pomiarowego;
    g) wykaz osób wykonujących samodzielne funkcje przy realizacji prac geodezyjnych wraz z informacją o wymaganych uprawnieniach;
    h) nawiązanie wodowskazów do właściwych reperów, punktów osnowy oraz przyjętego układu wysokościowego;
    i) wykaz współrzędnych punktów pomiarowych, punktów montażowych oraz zera wodowskazów;
    j) obliczenia wysokości wodowskazów i wartości odniesienia dla czujników;
    k) wyniki pomiarów lustra wody wykonanych w czasie prac pomiarowych, jeżeli są wymagane dla kalibracji albo weryfikacji wskazań;
    l) szkice, fotografie, opisy lokalizacji i dokumentację umożliwiającą identyfikację punktów pomiarowych w terenie;
    m) zestawienie wartości niezbędnych do konfiguracji, kalibracji, kontroli i odbioru czujników hydrologicznych;

n) wskazanie zależności pomiędzy wartościami pomiarowymi czujników, zerem wodowskazu oraz układem wysokościowym;

o) wnioski i zalecenia eksploatacyjne dotyczące kontroli geodezyjnej, ponownej niwelacji i aktualizacji danych po zmianach w obiekcie mostowym albo w lokalizacji wodowskazowej.

4) Operat Techniczny musi być opracowany przez osoby posiadające wymagane uprawnienia zawodowe w zakresie geodezji i kartografii, w zakresie adekwatnym do rodzaju wykonywanych prac. Wyniki pomiarów muszą być odniesione do obowiązującego państwowego systemu odniesień przestrzennych oraz do układów wysokościowych wymaganych przez Zamawiającego dla eksploatacji systemu RIS i prezentacji danych wodowskazowych.

5) Operat Techniczny musi zostać przekazany Zamawiającemu przed przystąpieniem do końcowej kalibracji, testów odbiorowych i przekazania czujników hydrologicznych do eksploatacji. Akceptacja Operatu Technicznego przez Zamawiającego stanowi warunek odbioru czujników hydrologicznych i danych pomiarowych w lokalizacjach objętych opracowaniem.

6) W przypadku przebudowy, modernizacji, remontu, zmiany obciążenia, istotnej ingerencji w obiekt mostowy, zmiany miejsca montażu czujnika, wymiany konstrukcji wsporczej, wymiany czujnika albo wystąpienia zdarzenia mogącego wpływać na geometrię pomiaru Generalny Wykonawca zobowiązany jest wykonać aktualizację Operatu Technicznego albo opracować aneks do Operatu w zakresie niezbędnym do potwierdzenia poprawności wartości pomiarowych.

2.2.5. Badania gruntowo-wodne i geotechniczne warunki posadowienia

1) Generalny Wykonawca musi wykonać rozpoznanie podłoża gruntowego i warunków wodnych w zakresie niezbędnym do posadowienia wież, masztów, fundamentów, szaf outdoor, konstrukcji wsporczych, słupów, kanalizacji kablowej i innych elementów infrastruktury RIS.

2) Zakres rozpoznania musi obejmować co najmniej:

a) badania geotechniczne podłoża gruntowego;

b) ocenę warunków wodnych, w tym poziomu wód gruntowych i wpływu wezbrań;

c) ustalenie kategorii geotechnicznej obiektu;

d) określenie parametrów do projektowania fundamentów;

e) ocenę ryzyka osiadania, podmywania, utraty stateczności, oddziaływania mrozu, wibracji i obciążeń środowiskowych;

f) zalecenia dotyczące odwodnienia wykopów, zabezpieczenia robót ziemnych i ochrony istniejących obiektów hydrotechnicznych.

3) Generalny Wykonawca opracuje opinię geotechniczną, dokumentację badań podłoża gruntowego, projekt geotechniczny lub dokumentację geologiczno-inżynierską, jeżeli

będzie wymagana ze względu na kategorię geotechniczną, warunki lokalne lub wymagania organów.

2.2.6. Dokumentacja dla nowych wież antenowych VHF/AIS

1) Dla każdej nowej wieży antenowej systemów VHF/AIS Generalny Wykonawca opracuje kompletną dokumentację projektową obejmującą co najmniej:
   a) analizę lokalizacyjną i formalnoprawną;
   b) sprawdzenie zgodności lokalizacji z miejscowym planem zagospodarowania przestrzennego albo uzyskanie decyzji o lokalizacji inwestycji celu publicznego lub innej wymaganej decyzji planistycznej;
   c) mapę do celów projektowych;
   d) badania gruntowo-wodne i dokumentację geotechniczną;
   e) projekt zagospodarowania terenu;
   f) projekt architektoniczno-budowlany;
   g) projekt techniczny;
   h) projekty wykonawcze branży konstrukcyjnej, elektrycznej, teletechnicznej, telekomunikacyjnej, odgromowej i uziemiającej;
   i) projekt przyłącza elektroenergetycznego albo projekt zasilania z istniejącej instalacji, wraz z warunkami technicznymi i uzgodnieniami;
   j) projekt tras kablowych i kanalizacji kablowej;
   k) analizę kompatybilności elektromagnetycznej;
   l) analizę oddziaływania pól elektromagnetycznych;
   m) projekt oznakowania przeszkodowego dziennego i nocnego, jeżeli będzie wymagane;
   n) informację BIOZ;
   o) komplet wniosków, załączników, uzgodnień i decyzji niezbędnych do uzyskania pozwolenia na budowę albo dokonania skutecznego zgłoszenia robót, jeżeli dany zakres będzie podlegał zgłoszeniu.
2) Dokumentacja musi jednoznacznie określać gabaryty wieży, wysokość całkowitą, wysokości zawieszenia anten, układ anten, azymuty anten kierunkowych, strefy dostępu, sposób posadowienia, układ fundamentów, rozwiązania materiałowe, zabezpieczenia antykorozyjne, obciążenia, klasy ekspozycji, zasilanie, uziemienie, ochronę odgromową, ochronę przepięciową, trasy kablowe, lokalizację szaf i urządzeń, dostęp serwisowy, sposób wygrodzenia oraz rozwiązania zabezpieczające przed dostępem osób nieuprawnionych.
3) Generalny Wykonawca musi wykazać, że zaprojektowana lokalizacja i wysokość instalacji antenowych zapewniają wymagane pokrycie radiowe oraz nie powodują pogorszenia parametrów systemu VHF/AIS. W przypadku zmiany lokalizacji, wysokości zawieszenia anten, typu anten albo parametrów radiowych Generalny Wykonawca wykona

potwierdzająco-korygujące planowanie radiowe oraz przedstawi Zamawiającemu wyniki obliczeń zasięgowych i zakłóceniowych.

2.2.7. Dokumentacja rozbiórki istniejących wież, masztów i konstrukcji

1) Dla każdej rozbiórki istniejącej wieży, masztu, konstrukcji wsporczej albo elementu infrastruktury technicznej Generalny Wykonawca opracuje dokumentację rozbiórkową w zakresie wymaganym przepisami prawa i warunkami zarządcy obiektu.
2) Dokumentacja rozbiórki musi obejmować co najmniej:
   a) mapę lokalizacyjną;
   b) inwentaryzację konstrukcji i wyposażenia;
   c) rysunki poglądowe z zasadniczymi wymiarami;
   d) ocenę stanu technicznego;
   e) opis prac przygotowawczych;
   f) technologię rozbiórki i kolejność robót;
   g) sposób zabezpieczenia terenu i obiektów sąsiednich;
   h) zasady wyłączenia, demontażu i zabezpieczenia instalacji;
   i) wymagania BHP i ppoż.;
   j) sposób zagospodarowania materiałów i odpadów rozbiórkowych;
   k) identyfikację materiałów niebezpiecznych, jeżeli mogą wystąpić;
   l) wymagane zgłoszenie rozbiórki albo pozwolenie na rozbiórkę;
   m) uzgodnienia z właścicielem lub zarządcą obiektu.
3) Generalny Wykonawca ponosi odpowiedzialność za zapewnienie ciągłości pracy istniejących elementów systemu RIS w okresie prowadzenia robót rozbiórkowych. Każde czasowe wyłączenie urządzeń systemu RIS wymaga wcześniejszego uzgodnienia z Zamawiającym.

2.2.8. Dokumentacja wodnoprawna i wymagania wynikające z Prawa wodnego

1) Generalny Wykonawca musi przeprowadzić analizę wymagalności decyzji, zgód, ocen, pozwoleń i zgłoszeń wodnoprawnych dla wszystkich robót realizowanych na terenach wód, w pobliżu wód, na obiektach hydrotechnicznych, na obszarach szczególnego zagrożenia powodzią, na terenach stopni wodnych, śluz, jazów, nabrzeży oraz na nieruchomościach zarządzanych przez PGW Wody Polskie.
2) W zakresie wymaganym przepisami Generalny Wykonawca opracuje operaty wodnoprawne, karty informacyjne, analizy hydrauliczne, opisy techniczne i załączniki graficzne oraz uzyska:
   a) pozwolenia wodnoprawne;

b) zgody wodnoprawne;

c) oceny wodnoprawne;

d) zwolnienia albo odstępstwa od zakazów obowiązujących na obszarach szczególnego zagrożenia powodzią;

e) uzgodnienia z właściwymi jednostkami PGW Wody Polskie;

f) inne rozstrzygnięcia wymagane dla lokalizacji i realizacji robót.

3) Dokumentacja wodnoprawna musi uwzględniać wpływ planowanych robót na bezpieczeństwo powodziowe, stateczność i funkcjonowanie obiektów hydrotechnicznych, drożność urządzeń wodnych, eksploatację stopni wodnych, dostęp serwisowy PGW Wody Polskie, ochronę wód oraz ograniczenia prowadzenia robót w okresach wezbrań i prac utrzymaniowych zarządcy.

2.2.9. Wymagania PGW Wody Polskie dla lokalizacji wież antenowych VHF/AIS

1) Dla wszystkich wież radiowych, masztów, konstrukcji wsporczych, instalacji antenowych, szaf teletechnicznych, tras kablowych, zasilania, uziemienia, instalacji odgromowych i infrastruktury towarzyszącej sytuowanych na terenach stopni wodnych, śluz, jazów, obiektów hydrotechnicznych albo nieruchomości zarządzanych przez PGW Wody Polskie Generalny Wykonawca musi uzyskać wszystkie wymagane zgody, uzgodnienia i warunki realizacyjne PGW Wody Polskie.

2) Wymóg dotyczy w szczególności lokalizacji: Śluza Brzeg Dolny, Śluza Rędzin, Śluza Szczytniki, Śluza Bartoszowice, Śluza Brzeg, teren Nadzoru Wodnego Opole oraz każdej lokalizacji zamiennej wskazanej przez Generalnego Wykonawcę, jeżeli zostanie ona usytuowana na terenie stopnia wodnego, śluzy, jazu, obiektu hydrotechnicznego lub nieruchomości zarządzanej przez PGW Wody Polskie.

3) Generalny Wykonawca opracuje i przedłoży właściwym jednostkom PGW Wody Polskie oraz Zamawiającemu kompletne projekty zagospodarowania terenu, projekty architektoniczno-budowlane, projekty techniczne, projekty wykonawcze i dokumentację uzgodnieniową dla planowanych wież radiowych oraz infrastruktury towarzyszącej.

4) Dokumentacja projektowa dla PGW Wody Polskie musi przedstawiać rzeczywiste rozwiązania materiałowe, konstrukcyjne, instalacyjne i lokalizacyjne, w szczególności:

a) gabaryty wieży;

b) sposób posadowienia;

c) rzędne wysokościowe;

d) wysokości zawieszenia anten;

e) schemat montażu anten;

f) przebieg tras kablowych;

g) sposób zasilania;

h) uziemienie;

i) ochronę odgromową i przepięciową;

j) lokalizację szaf i urządzeń;

k) dostęp serwisowy;

l) zabezpieczenie terenu;

m) wpływ robót i eksploatacji infrastruktury RIS na funkcjonowanie obiektu hydrotechnicznego.

5) Generalny Wykonawca opracuje dla każdej wieży radiowej sytuowanej na terenie PGW Wody Polskie ekspertyzę potwierdzającą brak negatywnego oddziaływania infrastruktury RIS na ludzi oraz inne systemy funkcjonujące na terenie stopnia wodnego, obiektu hydrotechnicznego lub w jego otoczeniu.

6) Ekspertyza musi obejmować co najmniej:

a) identyfikację wszystkich elementów infrastruktury RIS objętych oceną;

b) identyfikację systemów istniejących na terenie stopnia wodnego lub obiektu hydrotechnicznego;

c) ocenę oddziaływania pól elektromagnetycznych na ludzi w miejscach dostępnych dla ludności, personelu obsługi i ekip serwisowych;

d) ocenę kompatybilności elektromagnetycznej infrastruktury RIS z systemami istniejącymi;

e) ocenę ryzyka zakłóceń pracy systemów automatyki, sterowania, telemetrii, monitoringu, łączności, kontroli dostępu, zasilania, zabezpieczeń i systemów hydrotechnicznych;

f) ocenę wpływu instalacji antenowych, tras kablowych, zasilania, uziemienia i ochrony odgromowej na istniejącą infrastrukturę techniczną;

g) wskazanie środków eliminujących albo ograniczających ryzyko oddziaływania;

h) jednoznaczną konkluzję dotyczącą braku negatywnego oddziaływania infrastruktury RIS na ludzi oraz inne systemy przy zachowaniu przyjętych parametrów technicznych i organizacyjnych;

i) wykaz danych wejściowych, norm, przepisów, dokumentów, pomiarów, obliczeń i założeń wykorzystanych do sporządzenia ekspertyzy.

7) Generalny Wykonawca musi uzgodnić z PGW Wody Polskie oraz Zamawiającym zakres danych wejściowych do ekspertyzy, w tym wykaz systemów funkcjonujących na terenie stopnia wodnego lub obiektu hydrotechnicznego, które mają zostać objęte oceną. Jeżeli PGW Wody Polskie wskaże dodatkowe systemy, urządzenia, pomieszczenia, strefy pracy albo scenariusze eksploatacyjne wymagające oceny, Generalny Wykonawca uwzględni je w ekspertyzie bez dodatkowych roszczeń wobec Zamawiającego.

8) Generalny Wykonawca nie rozpocznie robót budowlanych, montażowych ani instalacyjnych dotyczących wieży radiowej na terenie PGW Wody Polskie przed:

a) opracowaniem kompletnej dokumentacji projektowej;

b) opracowaniem ekspertyzy o braku negatywnego oddziaływania infrastruktury RIS na ludzi oraz inne systemy;

c) przekazaniem dokumentacji i ekspertyzy Zamawiającemu;

d) uzyskaniem akceptacji Zamawiającego;

e) uzyskaniem wymaganej zgody PGW Wody Polskie;

f) uzyskaniem innych wymaganych decyzji, opinii, uzgodnień i pozwoleń.

9) Komplet dokumentacji projektowej, ekspertyza, korespondencja uzgodnieniowa, zgody PGW Wody Polskie oraz potwierdzenie spełnienia warunków wskazanych przez zarządcę terenu stanowią element dokumentacji odbiorowej danej lokalizacji. Brak któregokolwiek z tych dokumentów stanowi podstawę do odmowy odbioru robót w danej lokalizacji.

2.2.10. Montaż kamer, wodowskazów i czujników na istniejących obiektach hydrotechnicznych

1) Dla montażu kamer, wodowskazów, czujników hydrologicznych, czujników meteorologicznych, szaf, urządzeń transmisyjnych, anten, tras kablowych i urządzeń zasilających na istniejących obiektach hydrotechnicznych Generalny Wykonawca opracuje dokumentację projektową w zakresie wymaganym przez przepisy prawa, zarządcę obiektu i Zamawiającego.

2) Dokumentacja musi obejmować co najmniej:

a) mapę do celów projektowych albo inne materiały geodezyjne wymagane dla danej lokalizacji;

b) inwentaryzację obiektu i istniejących instalacji;

c) ocenę możliwości montażu urządzeń bez naruszenia konstrukcji i funkcji obiektu;

d) projekt mocowań i elementów wsporczych;

e) projekt tras kablowych;

f) projekt zasilania;

g) projekt instalacji teletechnicznych;

h) projekt uziemienia, ochrony odgromowej i ochrony przepięciowej;

i) operat wodnoprawny i pozwolenie wodnoprawne albo potwierdzenie braku wymagalności;

j) zwolnienie z zakazów obowiązujących na obszarach szczególnego zagrożenia powodzią, jeżeli jest wymagane;

k) uzgodnienia z PGW Wody Polskie albo innym zarządcą obiektu;

l) warunki prowadzenia robót w czynnym obiekcie hydrotechnicznym.

3) Dokumentacja musi zapewniać zachowanie ciągłości eksploatacji obiektu hydrotechnicznego, bezpieczeństwo użytkowników i personelu, brak negatywnego wpływu na pracę urządzeń hydrotechnicznych oraz możliwość późniejszego serwisu urządzeń RIS bez ingerencji w podstawowe funkcje obiektu.

2.2.11. Montaż infrastruktury RIS na obiektach mostowych, drogowych i kolejowych

1) Dla urządzeń instalowanych na obiektach mostowych, drogowych i kolejowych Generalny Wykonawca musi opracować dokumentację projektową i uzgodnieniową zgodną z wymaganiami zarządcy obiektu, zarządcy drogi, zarządcy infrastruktury kolejowej, gestorów sieci oraz właściwych organów.
2) Dokumentacja musi obejmować w szczególności:
   a) inwentaryzację obiektu, konstrukcji, instalacji i dostępnych tras kablowych;
   b) ocenę nośności i możliwości montażu urządzeń;
   c) projekt uchwytów, wsporników, obejm i konstrukcji mocujących;
   d) projekt tras kablowych po obiekcie;
   e) projekt zasilania i telekomunikacji;
   f) uzgodnienia z zarządcą obiektu;
   g) uzgodnienia z gestorami sieci;
   h) decyzje dotyczące pasa drogowego, lokalizacji urządzeń w pasie drogowym i zajęcia pasa drogowego, jeżeli są wymagane;
   i) projekt czasowej organizacji ruchu, jeżeli roboty będą wpływać na ruch drogowy, pieszy, rowerowy, kolejowy albo żeglugowy;
   j) uzgodnienia z właściwymi służbami utrzymaniowymi i eksploatacyjnymi;
   k) dokumentację zabezpieczeń antykorozyjnych i odtworzeniowych;
   l) instrukcję prowadzenia robót w czynnym obiekcie.
3) Generalny Wykonawca nie może wykonywać wierceń, kotwień, przewiertów, spawania, cięcia, prowadzenia tras kablowych ani innych ingerencji w elementy konstrukcyjne obiektu bez pisemnej zgody zarządcy obiektu i bez rozwiązań projektowych zatwierdzonych przez właściwe osoby posiadające wymagane uprawnienia.

2.2.12. Projekty przyłączy elektroenergetycznych, zasilania i tras kablowych

1) Generalny Wykonawca musi uzyskać warunki przyłączenia albo warunki zasilania dla wszystkich lokalizacji wymagających nowego lub zmodyfikowanego zasilania elektroenergetycznego.
2) Zakres projektów przyłączeniowych i zasilających obejmuje w szczególności:
   a) analizę zapotrzebowania mocy;
   b) uzyskanie warunków przyłączenia;
   c) uzgodnienie punktu przyłączenia;
   d) projekt przyłącza elektroenergetycznego;
   e) projekt wewnętrznej linii zasilającej;

f) projekt układu pomiarowego;

g) projekt rozdzielnic, zabezpieczeń i ochrony przeciwporażeniowej;

h) projekt zasilania gwarantowanego, jeżeli jest wymagane;

i) projekt uziemienia, ochrony odgromowej i ochrony przepięciowej;

j) projekt tras kablowych i kanalizacji kablowej;

k) uzgodnienia z właścicielami gruntów, zarządcami dróg, zarządcami mostów, PGW Wody Polskie, gminami, GDDKiA, PKP PLK albo innymi właściwymi podmiotami;

l) uzgodnienie na naradzie koordynacyjnej, jeżeli jest wymagane;

m) decyzje dotyczące lokalizacji urządzeń i zajęcia pasa drogowego, jeżeli są wymagane;

n) operat wodnoprawny i pozwolenie wodnoprawne, jeżeli zakres robót tego wymaga.

3) W przypadku prowadzenia przyłączy, kabli albo kanalizacji kablowej po obiekcie mostowym Generalny Wykonawca musi uzyskać od zarządcy obiektu warunki prowadzenia instalacji, warunki montażu uchwytów, dopuszczalne obciążenia, wymagania antykorozyjne, wymagania odtworzeniowe oraz warunki prowadzenia prac.

2.2.13. Uzgodnienia konserwatorskie i archeologiczne

1) Generalny Wykonawca musi ustalić, czy lokalizacje objęte Zamówieniem znajdują się na obszarach lub przy obiektach objętych ochroną konserwatorską, wpisem do rejestru zabytków, ujęciem w wojewódzkiej lub gminnej ewidencji zabytków, strefą ochrony konserwatorskiej albo strefą obserwacji archeologicznej.
2) W zakresie wynikającym z przepisów Generalny Wykonawca opracuje wymagane dokumenty i uzyska opinie, zalecenia, uzgodnienia, pozwolenia konserwatorskie oraz pozwolenia na prowadzenie badań archeologicznych albo nadzoru archeologicznego.
3) Roboty w rejonach wskazanych przez właściwego konserwatora zabytków Generalny Wykonawca przeprowadzi zgodnie z warunkami konserwatorskimi, pod wymaganym nadzorem konserwatorskim lub archeologicznym.
4) Koszty opracowań, uzgodnień, decyzji, nadzorów, badań i dokumentacji konserwatorskiej oraz archeologicznej Generalny Wykonawca ujmie w cenie oferty.

2.2.14. Inwentaryzacja zieleni i ochrona przyrody

1) Generalny Wykonawca musi wykonać inwentaryzację zieleni w zakresie niezbędnym do realizacji Przedmiotu Zamówienia, w szczególności dla lokalizacji wież, fundamentów, placów montażowych, dróg dojazdowych, tras kablowych, przyłączy i miejsc montażu urządzeń.
2) Inwentaryzacja zieleni musi obejmować identyfikację drzew, krzewów, zadrzewień, roślinności chronionej oraz potencjalnych siedlisk gatunków chronionych, jeżeli mogą zostać objęte oddziaływaniem robót.

3) Generalny Wykonawca uzyska wymagane zgody na usunięcie drzew lub krzewów, wniesie wymagane opłaty, wykona nasadzenia zastępcze lub kompensację przyrodniczą, jeżeli zostaną nałożone, oraz przeprowadzi wycinkę i zagospodarowanie biomasy zgodnie z decyzjami i przepisami.
4) Roboty muszą być projektowane i prowadzone z zachowaniem w maksymalnym możliwym stopniu istniejącego zadrzewienia. Generalny Wykonawca musi zachować okazy ustanowione pomnikami przyrody oraz uwzględnić wymagania dotyczące ochrony gatunkowej.

2.2.15. Raporty, opinie i ekspertyzy z zakresu ochrony środowiska

1) Generalny Wykonawca musi ustalić, czy planowane roboty, obiekty lub instalacje wymagają uzyskania decyzji o środowiskowych uwarunkowaniach, sporządzenia karty informacyjnej przedsięwzięcia, raportu o oddziaływaniu przedsięwzięcia na środowisko, przeprowadzenia oceny oddziaływania na obszar Natura 2000 albo innych opracowań środowiskowych.
2) Generalny Wykonawca opracuje i uzyska wszystkie wymagane raporty, opinie, ekspertyzy, analizy i decyzje z zakresu ochrony środowiska, w szczególności dotyczące:
   a) oddziaływania na wody powierzchniowe i podziemne;
   b) oddziaływania na obszary chronione, w tym Natura 2000;
   c) oddziaływania na gatunki chronione;
   d) emisji hałasu;
   e) oddziaływania pól elektromagnetycznych;
   f) gospodarki odpadami;
   g) zanieczyszczeń gruntu i wód;
   h) wpływu robót na żeglugę i eksploatację obiektów hydrotechnicznych;
   i) wpływu robót na bezpieczeństwo użytkowników terenów publicznych.
3) Generalny Wykonawca wykona pomiary ruchu drogowego, hałasu, pól elektromagnetycznych, drgań lub innych uciążliwości, jeżeli będą wymagane przez przepisy, organy, zarządców obiektów albo będą niezbędne do uzyskania decyzji i pozwoleń.

2.2.16. Inwentaryzacja i ekspertyzy istniejących obiektów budowlanych

1) Generalny Wykonawca musi wykonać inwentaryzację istniejących obiektów budowlanych, urządzeń, instalacji, konstrukcji, fundamentów, szaf, masztów, wież, tras kablowych i elementów infrastruktury, jeżeli będą wykorzystywane, przebudowywane, rozbudowywane, remontowane, rozbierane albo mogą zostać objęte oddziaływaniem robót.

2) Inwentaryzacja musi obejmować część architektoniczną, konstrukcyjną, instalacyjną, elektryczną, teletechniczną i technologiczną w zakresie niezbędnym do projektowania.
3) Generalny Wykonawca wykona ekspertyzy techniczne istniejących obiektów, jeżeli projektowane roboty obejmują montaż urządzeń na obiektach mostowych, hydrotechnicznych, budynkach, wieżach, masztach, konstrukcjach wsporczych albo innych obiektach, których nośność, stan techniczny lub sposób użytkowania mogą mieć wpływ na bezpieczeństwo robót i eksploatacji.
4) Ekspertyzy muszą potwierdzić możliwość montażu projektowanych urządzeń, uchwytów, anten, tras kablowych i szaf bez pogorszenia bezpieczeństwa, trwałości, użytkowania i utrzymania obiektu.

2.2.17. Porozumienia, zgody, pozwolenia oraz warunki techniczne i realizacyjne

1) Generalny Wykonawca musi uzyskać wszystkie porozumienia, zgody, pozwolenia, warunki techniczne i warunki realizacyjne związane z:
   a) dostępem do nieruchomości;
   b) prawem do dysponowania nieruchomością na cele budowlane;
   c) lokalizacją infrastruktury RIS na cudzych nieruchomościach;
   d) korzystaniem z obiektów mostowych, hydrotechnicznych, drogowych i kolejowych;
   e) prowadzeniem tras kablowych;
   f) budową lub przebudową przyłączy;
   g) zasilaniem elektroenergetycznym;
   h) transmisją danych;
   i) lokalizacją urządzeń w pasie drogowym;
   j) prowadzeniem robót na terenach kolejowych;
   k) prowadzeniem robót na terenach wodnych i obiektach hydrotechnicznych;
   l) zajęciem terenu na czas budowy;
   m) wejściem w teren i dostępem serwisowym;
   n) czasową organizacją ruchu;
   o) wyłączeniami albo ograniczeniami eksploatacyjnymi.
2) Generalny Wykonawca musi uzyskać warunki techniczne od gestorów sieci oraz uzgodnić projektowane rozwiązania z właścicielami lub zarządcami istniejących sieci, urządzeń i obiektów.
3) Jeżeli Zamawiający przekaże istniejące porozumienia, zgody, pozwolenia lub warunki techniczne, Generalny Wykonawca musi zweryfikować ich aktualność, zakres, terminy obowiązywania i przydatność do realizacji Przedmiotu Zamówienia. W razie potrzeby Generalny Wykonawca uzyska nowe albo zaktualizowane dokumenty.

4) Koszt uzyskania, aktualizacji i wykonania warunków, zgód, uzgodnień i pozwoleń Generalny Wykonawca ujmie w cenie oferty.

2.2.18. Pozwolenia radiowe, analizy radiowe i oddziaływanie pól elektromagnetycznych

1) Generalny Wykonawca musi opracować dokumentację i wykonać czynności niezbędne do uzyskania lub aktualizacji pozwoleń radiowych dla stacji VHF, AIS, DGNSS i innych urządzeń radiowych objętych Przedmiotem Zamówienia, jeżeli taki obowiązek wynika z przepisów albo przyjętej konfiguracji systemu.
2) Generalny Wykonawca musi opracować analizy radiowe, obliczenia zasięgowe, analizy zakłóceniowe, analizy kompatybilności elektromagnetycznej, analizy separacji anten oraz analizy oddziaływania pól elektromagnetycznych w zakresie wymaganym do zaprojektowania i uzgodnienia infrastruktury radiowej.
3) Minimalne odległości separacyjne pomiędzy antenami AIS, VHF, GPS, DGNSS oraz antenami innych systemów muszą zostać określone w projekcie wykonawczym na podstawie analizy kompatybilności elektromagnetycznej, zaleceń producentów urządzeń i warunków lokalizacyjnych.
4) Generalny Wykonawca musi wykonać wymagane zgłoszenia, pomiary albo sprawozdania dotyczące pól elektromagnetycznych, jeżeli będą wymagane przez przepisy, organy administracji, PGW Wody Polskie, zarządców obiektów albo Zamawiającego.

2.2.19. Oznakowanie przeszkodowe i uwarunkowania lotnicze

1) Generalny Wykonawca musi ustalić, czy projektowane wieże, maszty, anteny albo inne elementy infrastruktury RIS stanowią przeszkody lotnicze albo urządzenia wymagające oznakowania, zgłoszenia, uzgodnienia lub zastosowania szczególnych zabezpieczeń.
2) Analiza musi obejmować w szczególności:
   a) wysokość obiektu;
   b) rzędną terenu;
   c) sąsiedztwo lotnisk, lądowisk i lądowisk przyszpitalnych;
   d) powierzchnie ograniczające przeszkody;
   e) wymagania dotyczące oznakowania dziennego i nocnego;
   f) wymagania dotyczące zasilania i nadzoru oznakowania przeszkodowego;
   g) obowiązki zgłoszeniowe wobec właściwych organów i instytucji.
3) Jeżeli oznakowanie przeszkodowe jest wymagane, Generalny Wykonawca zaprojektuje, uzgodni, dostarczy, zamontuje, uruchomi i udokumentuje oznakowanie dzienne i nocne, a także zapewni jego zasilanie, zabezpieczenie i monitoring.
4) W szczególności Generalny Wykonawca musi uwzględnić wymagania dla lokalizacji Koźle Południe Ostrówek, znajdującej się w pobliżu lądowiska przyszpitalnego H328, dla

której w toku uzgodnień wskazano konieczność oznakowania przeszkodowego dziennego i nocnego. Raport uzgodnień wskazuje tę lokalizację jako wymagającą oznakowania zgodnego z przepisami o przeszkodach lotniczych, a aktualny tekst jednolity rozporządzenia w tym zakresie został ogłoszony w 2025 r.

2.2.20. Dokumentacja dla robót w czynnym systemie RIS i na czynnych obiektach

1) Generalny Wykonawca musi opracować harmonogram i technologię prowadzenia robót w sposób zapewniający ciągłość pracy istniejącego systemu RIS oraz ciągłość eksploatacji obiektów, na których prowadzone będą roboty.
2) Dokumentacja musi wskazywać:
   a) zakres robót wykonywanych przy czynnych urządzeniach;
   b) wymagane czasowe wyłączenia;
   c) procedury przełączeń i powrotu do konfiguracji podstawowej;
   d) zabezpieczenia przed utratą danych i przerwą transmisji;
   e) wymagania dotyczące prac na wysokości;
   f) wymagania dotyczące dostępu do obiektów;
   g) uzgodnienia z użytkownikami i zarządcami;
   h) procedury awaryjne;
   i) odpowiedzialność osób pełniących funkcje techniczne;
   j) sposób dokumentowania wykonania robót.
3) Każde wyłączenie lub ograniczenie pracy istniejącego elementu systemu RIS wymaga wcześniejszej akceptacji Zamawiającego.

2.2.21. Lokalizacje zamienne

1) Jeżeli realizacja infrastruktury RIS w lokalizacji wskazanej w PFU, Planie VHF/AIS, Planie CCTV, Planie połączeń transmisyjnych albo dokumentach uzgodnieniowych okaże się niemożliwa, istotnie utrudniona, nieuzasadniona technicznie albo nieuzgodniona przez właściwego zarządcę, Generalny Wykonawca wytypuje lokalizację zamienną.
2) Lokalizacja zamienna musi zapewniać równoważne albo lepsze parametry funkcjonalne, techniczne, radiowe, transmisyjne, obserwacyjne, eksploatacyjne i formalnoprawne względem lokalizacji pierwotnej.
3) Generalny Wykonawca musi przedstawić dla lokalizacji zamiennej:
   a) analizę formalnoprawną;
   b) analizę własnościową;
   c) potwierdzenie możliwości uzyskania prawa do dysponowania nieruchomością;

d) analizę techniczną;

e) obliczenia zasięgowe lub widokowe, jeżeli dotyczą lokalizacji radiowej albo kamerowej;

f) analizę transmisyjną;

g) analizę zasilania;

h) analizę środowiskową;

i) analizę kosztową;

j) harmonogram uzyskania wymaganych zgód;

k) projekt wymaganych zmian w dokumentacji.

4) Lokalizacja zamienna wymaga akceptacji Zamawiającego przed rozpoczęciem procedur administracyjnych i projektowania szczegółowego.

2.2.22. Dokumentacja odbiorowa, powykonawcza i eksploatacyjna

1) Generalny Wykonawca musi opracować i przekazać Zamawiającemu dokumentację odbiorową i powykonawczą dla każdego obiektu, lokalizacji i zakresu branżowego.

2) Dokumentacja odbiorowa musi obejmować co najmniej:

a) zatwierdzoną dokumentację projektową;

b) decyzje administracyjne, pozwolenia, zgody, uzgodnienia i warunki;

c) protokoły narad koordynacyjnych;

d) protokoły odbiorów branżowych;

e) protokoły pomiarów elektrycznych, uziemienia, ochrony odgromowej i ochrony przeciwporażeniowej;

f) protokoły pomiarów torów antenowych;

g) protokoły konfiguracji urządzeń;

h) protokoły testów funkcjonalnych i integracyjnych;

i) dokumentację fotograficzną;

j) geodezyjną inwentaryzację powykonawczą;

k) instrukcje eksploatacji i konserwacji;

l) karty katalogowe, deklaracje zgodności, certyfikaty i dokumenty dopuszczające;

m) potwierdzenie spełnienia wymagań zarządców terenów i obiektów;

n) komplet dokumentów wymaganych do zawiadomienia o zakończeniu budowy albo uzyskania pozwolenia na użytkowanie, jeżeli będą wymagane.

3) W przypadku lokalizacji na terenach PGW Wody Polskie dokumentacja odbiorowa musi zawierać także zgodę PGW Wody Polskie, ekspertyzę o braku negatywnego oddziaływania infrastruktury RIS na ludzi i inne systemy, dokumentację uzgodnieniową oraz potwierdzenie wykonania warunków wskazanych przez PGW Wody Polskie.

2.2.23. Dodatkowe wytyczne inwestorskie i uwarunkowania związane z finansowaniem

1) Zamówienie będzie realizowane ze środków publicznych, w tym ze środków Funduszu Spójności w ramach Programu Fundusze Europejskie na Infrastrukturę, Klimat, Środowisko 2021-2027 w ramach projektu „Rozbudowa systemu RIS na Odrzańskiej Drodze Wodnej” (numer projektu FENX.04.04-IP.02-0001/24).
2) Generalny Wykonawca musi uwzględnić wymagania dotyczące kwalifikowalności wydatków, trwałości projektu, oznakowania inwestycji, dokumentowania robót, archiwizacji dokumentów, kontroli, audytu oraz udostępniania dokumentacji instytucjom uprawnionym do kontroli.
3) Dokumentacja projektowa, odbiorowa i powykonawcza musi być prowadzona w sposób umożliwiający jednoznaczne przypisanie wykonanych robót, dostaw, usług, urządzeń, licencji i czynności do zakresu rzeczowego projektu oraz do właściwych lokalizacji systemu RIS.
4) Generalny Wykonawca musi oznakować produkty projektu, miejsca realizacji robót, dostarczone urządzenia, wyposażenie, dokumentację, materiały informacyjne, instrukcje, oprogramowanie, interfejsy użytkownika oraz inne rezultaty Przedmiotu Zamówienia zgodnie z aktualnymi na dzień wykonania oznakowania wytycznymi, podręcznikami, zasadami komunikacji marki, księgą identyfikacji wizualnej oraz wymaganiami dotyczącymi informacji i promocji właściwymi dla programu Fundusze Europejskie na Infrastrukturę, Klimat, Środowisko 2021–2027, Funduszu Spójności oraz umowy o dofinansowanie projektu.
5) Oznakowanie musi jednoznacznie komunikować, że projekt jest dofinansowany przez Unię Europejską ze środków Funduszu Spójności w ramach programu Fundusze Europejskie na Infrastrukturę, Klimat, Środowisko 2021–2027. Generalny Wykonawca musi stosować wymagane zestawienie znaków, w szczególności znak Funduszy Europejskich, znak barw Rzeczypospolitej Polskiej oraz znak Unii Europejskiej wraz z właściwym sformułowaniem dotyczącym dofinansowania, w układzie, proporcjach, kolorystyce, polach ochronnych i minimalnych wielkościach zgodnych z aktualnymi wytycznymi.
6) Generalny Wykonawca musi zapewnić oznakowanie co najmniej:
    a) dokumentacji projektowej, wykonawczej, powykonawczej, odbiorowej, testowej, eksploatacyjnej i szkoleniowej;
    b) prezentacji, raportów, harmonogramów, protokołów, instrukcji, procedur, materiałów warsztatowych i szkoleniowych;
    c) miejsc realizacji robót, w tym przez zastosowanie wymaganych tablic, plakatów albo innych nośników informacji, jeżeli obowiązek ich zastosowania wynika z wytycznych;
    d) sprzętu, urządzeń, wyposażenia, szaf, zestawów komputerowych, elementów infrastruktury teleinformatycznej, urządzeń terenowych, elementów systemów CCTV, VHF/AIS, transmisji danych, zasilania oraz infrastruktury serwerowej, o ile ich oznakowanie jest wymagane albo technicznie możliwe;

e) aplikacji, portali, interfejsów, ekranów startowych, paneli administracyjnych i innych produktów cyfrowych wykonanych lub zmodyfikowanych w ramach Zamówienia;

f) materiałów publikowanych w formie elektronicznej, w tym plików PDF, dokumentów DOCX, XLSX, prezentacji, materiałów graficznych oraz treści przekazywanych Zamawiającemu do publikacji.

7) Oznakowanie sprzętu i wyposażenia musi zostać wykonane w sposób trwały, estetyczny, czytelny, odporny na warunki eksploatacji oraz niepowodujący utraty gwarancji producenta, pogorszenia bezpieczeństwa użytkowania, ograniczenia dostępu serwisowego ani naruszenia wymagań technicznych urządzeń. Aktualny podręcznik dla beneficjentów Funduszy Europejskich wskazuje obowiązek oznaczania wyposażenia, sprzętu i środków transportu powstałych lub zakupionych w projekcie dofinansowanym z Funduszy Europejskich.

8) Generalny Wykonawca przedstawi Zamawiającemu do akceptacji propozycję sposobu oznakowania produktów projektu, obejmującą co najmniej wykaz produktów podlegających oznakowaniu, rodzaj oznakowania, lokalizację oznakowania, projekt graficzny, format, rozmiar, technikę wykonania, trwałość oraz termin montażu albo naniesienia oznakowania. Generalny Wykonawca może zastosować oznakowanie dopiero po uzyskaniu akceptacji Zamawiającego.

9) Generalny Wykonawca musi wykonać i przekazać Zamawiającemu dokumentację potwierdzającą wykonanie obowiązków informacyjno-promocyjnych, w szczególności dokumentację fotograficzną oznakowanych miejsc, urządzeń i wyposażenia, wykaz oznakowanych produktów projektu oraz kopie materiałów i dokumentów zawierających wymagane oznakowanie.

10) Koszt opracowania projektów graficznych, wykonania, dostawy, montażu, utrzymania, uzupełnienia, wymiany albo poprawienia oznakowania produktów projektu oraz koszt dokumentowania spełnienia obowiązków informacyjno-promocyjnych Generalny Wykonawca musi ująć w cenie oferty

3. Spis tabel

Tabela 1: Wykaz nowych wież antenowych stacji radiokomunikacyjnych VHF/AIS wraz z funkcją DGNSS, czujników meteorologicznych oraz kamer obserwacyjnych i dozorowych *21*
Tabela 2: Wykaz nowych lokalizacji monitoringu wizyjnego oraz stacji czujników hydrologicznych *24*
Tabela 3: Wykaz obiektów infrastruktury systemu RIS objętych wymianą obecnych urządzeń i elementów *26*
Tabela 4: Zbiorcze zestawienie nowych lokalizacji systemu RIS oraz och funkcji *38*
Tabela 5: Numery seryjne serwerów Dell EMC PowerEdge MX740c *185*
Tabela 6: Wykaz lokalizacji czujników objętych integracją *266*
Tabela 7: Wykaz stosowanych skrótów, skrótowców i pojęć *394*

4. Spis rysunków

Rysunek 1: Przykładowa konstrukcja nośna szafy wraz z podestem (Lokalizacja Świerkocin) 136
Rysunek 2: Przykładowa konstrukcja nośna szafy wraz z systemem poziomowania (Lokalizacja Świerkocin) 136
Rysunek 3: Rzut pomieszczenia 32 153
Rysunek 4: Kanały kablowe łączące pomieszczenia serwerowni 159
Rysunek 5: Kanały kablowe łączące pomieszczenia serwerowni 160
Rysunek 5: Schemat rozkładu pomieszczeń objętych modernizacją sieci teleinformatycznej 393

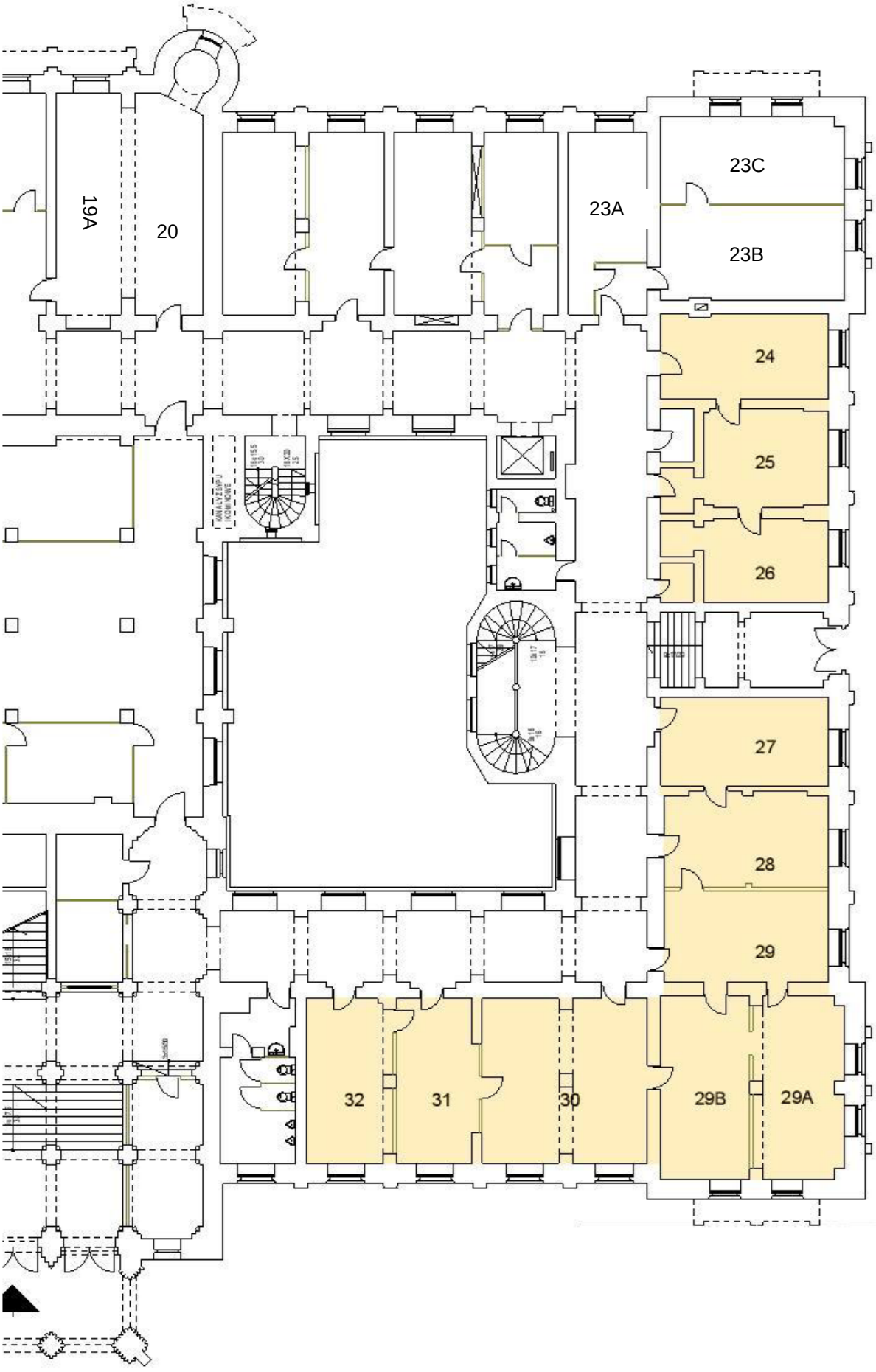
5. Załączniki

Wykaz załączników:

Załącznik nr 1 - Schemat rozkładu pomieszczeń objętych modernizacją sieci teleinformatycznej

Załącznik nr 2 – Wykaz stosowanych skrótów i pojęć

Załącznik nr 1 - Schemat rozkładu pomieszczeń objętych modernizacją sieci teleinformatycznej



Rysunek 6: Schemat rozkładu pomieszczeń objętych modernizacją sieci teleinformatycznej

Załącznik nr 2 – Wykaz stosowanych skrótów i pojęć

W poniższej tabeli przedstawiono definicje podstawowych pojęć oraz skrótowców wykorzystywanych w niniejszym dokumencie, które mogą mieć wpływ na lepsze i poprawne zrozumienie treści zawartej w dalszej części tego dokumentu.

Tabela 7: Wykaz stosowanych skrótów, skrótowców i pojęć

6J	Oznaczenie minimalnej liczby włókien światłowodowych w przyłączu światłowodowym, stosowane w PFU w odniesieniu do połączenia ośrodka zapasowego z Centrum RIS.
AIS	Automatic Identification System – system automatycznej identyfikacji statków. W systemie RIS wykorzystywany do pozyskiwania, przetwarzania i prezentacji informacji o jednostkach pływających, w tym ich pozycji, kursie, prędkości, identyfikatorze MMSI i innych danych nawigacyjnych.
API	Application Programming Interface – interfejs programistyczny umożliwiający wymianę danych pomiędzy systemami teleinformatycznymi. W PFU pojęcie stosowane m.in. w odniesieniu do integracji systemu RIS z EuRIS, Systemem Hydrologii IMGW-PIB oraz przyszłymi systemami zewnętrznymi.
ASCII	American Standard Code for Information Interchange – standard kodowania znaków, wskazywany w PFU jako jeden z możliwych formatów/protokołów komunikacji lokalnych komponentów akwizycji danych z czujnikami.
ASVS	Application Security Verification Standard – standard OWASP określający wymagania weryfikacji bezpieczeństwa aplikacji. W PFU może stanowić punkt odniesienia dla testów bezpieczeństwa aplikacji i usług cyfrowych.
BCP	Business Continuity Plan – Plan Ciągłości Działania. Dokument określający zasady utrzymania lub odtworzenia działania systemu RIS w przypadku awarii, zakłóceń, utraty dostępności komponentów albo innych zdarzeń wpływających na ciągłość usług.
BCP/DR	Łączne określenie wymagań dotyczących ciągłości działania oraz odtwarzania po awarii, obejmujące procedury, zasoby, mechanizmy techniczne i organizacyjne pozwalające utrzymać lub przywrócić działanie systemu RIS.
BHP	Bezpieczeństwo i higiena pracy. W PFU pojęcie dotyczy zasad prowadzenia robót, prac montażowych, serwisowych i eksploatacyjnych, w szczególności na obiektach budowlanych, wieżach, masztach, mostach, w serwerowniach i szafach teletechnicznych.
BKT	Nazwa producenta rozwiązań stosowanych w istniejącej infrastrukturze technicznej Zamawiającego, m.in. w zakresie elementów monitoringu środowiskowego, wentylacji, zasilania i wyposażenia szaf teletechnicznych. W PFU nazwa występuje jako opis stanu istniejącego lub punkt odniesienia dla kompatybilności.
CE	Oznakowanie zgodności wyrobu z wymaganiami prawodawstwa Unii Europejskiej dotyczącymi bezpieczeństwa, zdrowia i ochrony środowiska.

CESNI	Comité Européen pour l’Élaboration de Standards dans le Domaine de Navigation Intérieure – Europejski Komitet ds. opracowywania standardów w żegludze śródlądowej. Organizacja opracowująca m.in. standardy ES-RIS.
CCTV	Closed-Circuit Television – system monitoringu wizyjnego. W PFU oznacza podsystem kamer, rejestracji, transmisji, podglądu, zarządzania obrazem, masek prywatności, archiwizacji oraz udostępniania obrazu w ramach systemu RIS.
CCTV/VSS	Closed-Circuit Television / Video Surveillance System – system monitoringu wizyjnego / system dozoru wizyjnego. Pojęcie stosowane przy odniesieniach normatywnych do standardów dotyczących CCTV i VSS.
Centrum RIS	Centralna lokalizacja organizacyjna i techniczna systemu RIS, w której realizowane są funkcje operatorskie, nadzorcze, administracyjne, integracyjne, serwerowe oraz usługowe systemu informacji rzecznej.
CNA	Converged Network Adapter – karta sieciowa umożliwiająca obsługę ruchu sieciowego oraz, w zależności od konfiguracji, ruchu pamięci masowej. Pojęcie może występować w kontekście rozbudowy infrastruktury serwerowej.
CPD	Centrum Przetwarzania Danych – wydzielone środowisko techniczne przeznaczone do utrzymywania zasobów serwerowych, pamięci masowej, sieci, bezpieczeństwa, kopii zapasowych i usług systemowych.
CPU	Central Processing Unit – procesor. W PFU pojęcie odnosi się do zasobów obliczeniowych serwerów środowiska pracy systemu RIS.
CSIRT	Computer Security Incident Response Team – zespół reagowania na incydenty bezpieczeństwa komputerowego. W PFU pojęcie występuje w kontekście incydentów bezpieczeństwa, zgłaszania podatności i obowiązków wynikających z przepisów o cyberbezpieczeństwie.
DAC/AOC	Direct Attach Cable / Active Optical Cable – typy kabli stosowanych do szybkich połączeń sieciowych lub serwerowych, w szczególności w środowiskach centrum danych.
Data Center	Centrum danych lub zewnętrzny ośrodek przetwarzania danych, w którym mogą być kolokowane zasoby systemu RIS, w szczególności elementy ośrodka zapasowego.
DC	Data Center – centrum danych. Skrót stosowany zamiennie z pojęciem Data Center.
DGPS	Differential Global Positioning System – różnicowy GPS. Historycznie stosowane określenie technologii dystrybucji poprawek różnicowych dla GPS. W PFU może występować w odniesieniu do stanu istniejącego lub wcześniejszych wdrożeń RIS.
DGNSS	Differential Global Navigation Satellite System – różnicowy system nawigacji satelitarnej. W PFU oznacza funkcję dystrybucji poprawek różnicowych dla systemów GNSS w ramach infrastruktury radiowej RIS.
DIN	Deutsches Institut für Normung – niemiecka organizacja normalizacyjna. W PFU skrót pojawia się m.in. przy oznaczeniach szyn montażowych DIN stosowanych w instalacjach elektrycznych i teletechnicznych.
DK	Droga krajowa. Skrót stosowany przy opisie lokalizacji obiektów drogowych, w szczególności mostów i dróg, na których lub przy których planowana jest infrastruktura RIS.

DNSH	Do No Significant Harm – zasada „nie czyń poważnych szkód”. Zasada horyzontalna finansowania środkami UE, wymagająca, aby projekt nie powodował znaczących szkód dla celów środowiskowych.
Dokumentacja Administratora	Dokumentacja przeznaczona dla administratorów systemu RIS, opisująca konfigurację, zasady zarządzania, konta, role, uprawnienia, procedury administracyjne, diagnostyczne, utrzymaniowe i odtworzeniowe.
Dokumentacja eksploatacyjna	Dokumentacja opisująca zasady bieżącego użytkowania, utrzymania, konserwacji, testowania, diagnostyki, reagowania na awarie i aktualizacji systemu RIS oraz jego komponentów.
Dokumentacja powykonawcza	Dokumentacja odzwierciedlająca rzeczywisty sposób wykonania robót, dostaw, instalacji, konfiguracji i integracji systemu RIS po zakończeniu prac.
Dokumentacja projektowa	Dokumentacja opracowywana przez Generalnego Wykonawcę w formule „zaprojektuj i zbuduj”, obejmująca projekty, uzgodnienia, rozwiązania techniczne, lokalizacyjne, formalnoprawne i wykonawcze niezbędne do realizacji zamówienia.
Dokumentacja Użytkownika	Dokumentacja przeznaczona dla użytkowników końcowych i operatorów systemu RIS, opisująca sposób korzystania z funkcji systemu, usług cyfrowych, paneli administracyjnych, raportów i procedur operacyjnych.
DP4400	Dell EMC Avamar DP4400 / Integrated Data Protection Appliance / PowerProtect DP4400 – istniejące rozwiązanie Zamawiającego służące do ochrony danych i wykonywania kopii zapasowych, objęte w PFU zakresem rozbudowy.
DR	Disaster Recovery – odtwarzanie po awarii. Zbiór działań, procedur i mechanizmów technicznych służących przywróceniu działania systemu po awarii.
DRP	Disaster Recovery Plan – Plan Odtworzenia po Awarii. Dokument określający sposób odtworzenia systemu RIS, jego danych, konfiguracji, usług i infrastruktury po wystąpieniu awarii lub katastrofy.
DW	Droga wojewódzka. Skrót stosowany przy opisie lokalizacji obiektów drogowych, w szczególności mostów i dróg wojewódzkich powiązanych z lokalizacjami RIS.
ECDIS	Electronic Chart Display and Information System – system obrazowania elektronicznych map nawigacyjnych i informacji nawigacyjnej. W PFU pojęcie występuje w kontekście Inland ECDIS oraz obsługi map śródlądowych.
EMC	Electromagnetic Compatibility – kompatybilność elektromagnetyczna. W PFU pojęcie dotyczy zgodności urządzeń i instalacji z wymaganiami ograniczającymi emisję zakłóceń oraz zapewniającymi odporność na zakłócenia elektromagnetyczne.
ENC	Electronic Navigational Chart – elektroniczna mapa nawigacyjna. W PFU pojęcie występuje głównie w związku z Inland ENC i usługami VTT.
ERDMS	European Reference Data Management System – europejski system zarządzania danymi referencyjnymi, powiązany z usługami RIS, danymi referencyjnymi i interoperacyjnością.
ERI	Electronic Reporting International / Electronic Reporting for Inland Navigation – elektroniczne raportowanie statków w żegludze śródlądowej, jedna z usług RIS.
ES-RIS	European Standard for River Information Services – europejski standard usług informacji rzecznej opracowywany przez CESNI. W PFU jest jednym z podstawowych standardów odniesienia dla rozbudowy RIS.

ETA	Estimated Time of Arrival – szacowany czas przybycia. W PFU pojęcie występuje w kontekście funkcjonalności systemu VTT i obliczania przewidywanego czasu dotarcia jednostki do wskazanego miejsca.
Ethernet	Technologia sieciowa wykorzystywana do transmisji danych w sieciach LAN i środowiskach teleinformatycznych systemu RIS.
EuRIS	European River Information Services – europejska platforma/usługa informacji rzecznej umożliwiająca wymianę i udostępnianie danych RIS na poziomie europejskim.
FAT	Factory Acceptance Tests – testy akceptacyjne wykonywane przed dostawą albo przed wdrożeniem rozwiązania u Zamawiającego, jeżeli zostaną przewidziane dla danego komponentu.
Generalny Wykonawca	Podmiot wybrany w postępowaniu o udzielenie zamówienia publicznego, odpowiedzialny za zaprojektowanie, wykonanie, dostawę, konfigurację, integrację, testowanie, dokumentację, przekazanie do eksploatacji, gwarancję i utrzymanie przedmiotu zamówienia.
GIS	Geographic Information System – system informacji geograficznej. Pojęcie może być stosowane w kontekście danych przestrzennych, map, lokalizacji i analiz geograficznych systemu RIS.
GNSS	Global Navigation Satellite System – globalny system nawigacji satelitarnej, obejmujący m.in. GPS, Galileo, GLONASS i BeiDou. W PFU powiązany z funkcją DGNSS.
GPS	Global Positioning System – globalny system pozycjonowania satelitarnego. W PFU pojęcie występuje w kontekście lokalizacji, pomiarów i historycznych funkcji DGPS.
GUI	Graphical User Interface – graficzny interfejs użytkownika. W PFU pojęcie dotyczy interfejsów aplikacyjnych, paneli operatorskich, administracyjnych i usług cyfrowych.
HA	High Availability – wysoka dostępność. W PFU oznacza rozwiązania projektowe i techniczne ograniczające ryzyko niedostępności systemu, usług lub komponentów w przypadku awarii pojedynczego elementu.
HCL	Hardware Compatibility List – lista kompatybilności sprzętowej producenta oprogramowania lub platformy, wskazująca sprzęt wspierany dla danego rozwiązania.
HTTPS	Hypertext Transfer Protocol Secure – bezpieczny protokół komunikacji HTTP z użyciem szyfrowania TLS. W PFU stosowany w kontekście bezpiecznych usług, API i interfejsów administracyjnych.
ICT	Information and Communication Technologies – technologie informacyjno-komunikacyjne. W PFU pojęcie odnosi się do produktów, usług, systemów teleinformatycznych i komponentów infrastruktury cyfrowej.
IEC	International Electrotechnical Commission – Międzynarodowa Komisja Elektrotechniczna, organizacja opracowująca normy techniczne w obszarze elektrotechniki, elektroniki i technologii pokrewnych.
IEEE	Institute of Electrical and Electronics Engineers – organizacja opracowująca standardy techniczne, m.in. dla sieci komputerowych, Ethernet, PoE i technologii transmisji danych.

IENC / Inland ENC	Inland Electronic Navigational Chart – elektroniczna mapa nawigacyjna dla żeglugi śródlądowej. W PFU pojęcie występuje w kontekście usług VTT i obsługi śródlądowych map nawigacyjnych.
IHO	International Hydrographic Organization – Międzynarodowa Organizacja Hydrograficzna, opracowująca standardy dotyczące danych hydrograficznych i map elektronicznych.
IK	Klasa odporności mechanicznej obudowy, określająca odporność na uderzenia mechaniczne. W PFU stosowana m.in. przy wymaganiach dla szaf teletechnicznych.
IMGW-PIB	Instytut Meteorologii i Gospodarki Wodnej – Państwowy Instytut Badawczy. W PFU podmiot powiązany z usługą przekazywania danych z wodowskazów systemu RIS do Systemu Hydrologii.
Inland AIS	Odmiana systemu AIS dostosowana do żeglugi śródlądowej, wykorzystywana w usługach RIS do śledzenia i identyfikacji jednostek pływających.
Inland ECDIS	System obrazowania elektronicznych map nawigacyjnych i informacji nawigacyjnej dla żeglugi śródlądowej. W PFU punkt odniesienia dla obsługi map w systemie VTT.
IP	Internet Protocol – protokół sieciowy służący do adresowania i przesyłania danych w sieciach komputerowych. W PFU pojęcie występuje m.in. przy adresacji IP, sieci IP, kamerach IP, transmisji danych i VPN.
IP20 / IP55 / IP66	Stopnie ochrony obudowy przed dostępem do części niebezpiecznych, wnikaniem ciał obcych i wody. W PFU stosowane przy wymaganiach dla urządzeń, zasilaczy, sensorów i szaf teletechnicznych.
iSCSI	Internet Small Computer Systems Interface – protokół umożliwiający dostęp do zasobów pamięci masowej przez sieć IP. W PFU pojęcie stosowane w kontekście istniejących i rozbudowywanych zasobów storage.
ISO	International Organization for Standardization – Międzynarodowa Organizacja Normalizacyjna. W PFU pojęcie występuje w odniesieniu do norm zarządzania, bezpieczeństwa, jakości, dokumentacji i infrastruktury.
IT	Information Technology – technologie informatyczne. Pojęcie używane ogólnie dla systemów, infrastruktury, oprogramowania, usług i zasobów teleinformatycznych.
JSON	JavaScript Object Notation – tekstowy format wymiany danych. W PFU wskazywany m.in. przy integracji z Systemem Hydrologii IMGW-PIB i usługach API.
Kamera dozorowa	Kamera przeznaczona do nadzoru nad infrastrukturą techniczną systemu RIS, w szczególności wieżami, szafami teletechnicznymi, ogrodzeniami, strefami dostępu i miejscami instalacji urządzeń.
Kamera obserwacyjna	Kamera przeznaczona do obserwacji drogi wodnej, mostów, śluz, nabrzeży, obiektów hydrotechnicznych i innych miejsc istotnych dla nadzoru nad bezpieczeństwem żeglugi.
Kamera PTZ	Kamera obrotowa umożliwiająca zdalne sterowanie kierunkiem obserwacji oraz przybliżeniem obrazu. Skrót PTZ oznacza Pan-Tilt-Zoom.
Kamera stała	Kamera o zasadniczo stałym kierunku obserwacji, bez pełnej funkcji zdalnego obrotu i przybliżania w trybie PTZ.

Kanał wideo	Pojedyncze źródło obrazu obsługiwane przez system CCTV, np. kamera systemu RIS albo strumień wideo udostępniany przez inny podmiot.
KPŻ2030	Krajowy Program Żeglugowy do roku 2030 – dokument strategiczny dotyczący rozwoju żeglugi śródlądowej, powiązany z celami projektu RIS.
KRI	Krajowe Ramy Interoperacyjności – wymagania dotyczące interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
KSC	Krajowy System Cyberbezpieczeństwa – system organizacyjno-prawny określający wymagania i obowiązki w zakresie cyberbezpieczeństwa, wynikające z ustawy o krajowym systemie cyberbezpieczeństwa oraz przepisów powiązanych.
LAN	Local Area Network – lokalna sieć komputerowa. W PFU pojęcie odnosi się do sieci w serwerowniach, Centrum RIS, środowisku pracy systemu RIS i modernizowanej sieci teleinformatycznej.
LK	Linia kolejowa. Skrót stosowany przy opisie lokalizacji obiektów kolejowych, w szczególności mostów kolejowych.
LoS	Line of Sight – widoczność optyczna pomiędzy punktami radiowymi. Pojęcie stosowane w analizach radiowych i transmisyjnych.
LUN	Logical Unit Number – logiczny wolumen udostępniany przez macierz dyskową serwerom lub platformie wirtualizacyjnej.
LTE	Long Term Evolution – standard transmisji danych w sieciach komórkowych czwartej generacji, stosowany jako jedna z technologii dostępowych dla lokalizacji RIS.
LTE/5G	Technologie publicznych sieci komórkowych czwartej i piątej generacji, wykorzystywane lub analizowane jako tory transmisyjne dla lokalizacji systemu RIS.
Macierz dyskowa	Urządzenie pamięci masowej przeznaczone do centralnego składowania danych, udostępniania wolumenów serwerom, zapewniania ochrony danych, replikacji, wysokiej dostępności i współpracy ze środowiskiem wirtualizacyjnym.
MCM	Multi-Chassis Management lub grupa zarządzania wieloma obudowami/kasetami serwerowymi, używana w kontekście istniejącego środowiska Dell PowerEdge MX7000.
ME4024	Dell EMC PowerVault ME4024 – istniejąca macierz dyskowa Zamawiającego objęta w PFU wymaganiami dotyczącymi rozbudowy.
ME424	Dell EMC PowerVault ME424 – półka dyskowa kompatybilna z macierzą Dell EMC PowerVault ME4024, wskazywana w kontekście możliwej rozbudowy pojemności.
MMSI	Maritime Mobile Service Identity – morski numer identyfikacyjny jednostki lub stacji radiowej. W PFU wykorzystywany w kontekście identyfikacji jednostek AIS i wyszukiwania jednostek w systemie VTT.
NAS	Network Attached Storage – sieciowa pamięć masowa. W PFU pojęcie występuje w kontekście rozróżnienia zasobów pamięci masowej i zakresu dostaw.

NBD	Next Business Day – następny dzień roboczy. Parametr serwisowy oznaczający termin reakcji lub naprawy w następnym dniu roboczym, o ile zostanie przyjęty dla danego komponentu.
NMEA	National Marine Electronics Association – standard komunikacyjny wykorzystywany m.in. w urządzeniach nawigacyjnych i sensorach. W PFU wskazywany jako jeden z protokołów komunikacji lokalnych komponentów z czujnikami.
NR / 5G NR	New Radio – technologia radiowa piątej generacji sieci komórkowych. W PFU może występować w kontekście transmisji danych z wykorzystaniem sieci 5G.
NtS	Notices to Skippers – komunikaty dla kierowników statków. Jedna z usług RIS polegająca na udostępnianiu informacji istotnych dla żeglugi.
ODW	Odrzańska Droga Wodna – droga wodna stanowiąca obszar realizacji projektu rozbudowy systemu RIS.
ONVIF	Open Network Video Interface Forum – otwarty standard interoperacyjności urządzeń systemów wizyjnych IP. W PFU stosowany w kontekście kompatybilności kamer i systemów CCTV.
Operat Techniczny z pomiarów wodowskazów	Dokument geodezyjny zawierający dane dotyczące nawiązania wodowskazów, punktów odniesienia i poziomów, stanowiący podstawę poprawnego określenia wartości pomiarowych wodowskazów.
Ośrodek zapasowy	Lokalizacja zapasowa środowiska pracy systemu RIS, służąca zapewnieniu ciągłości działania, replikacji danych i odtworzenia usług po awarii lokalizacji podstawowej.
OWASP	Open Worldwide Application Security Project – organizacja i zestaw dobrych praktyk dotyczących bezpieczeństwa aplikacji, wykorzystywany jako punkt odniesienia dla bezpieczeństwa usług cyfrowych i API.
PDF	Portable Document Format – format plików elektronicznych, wskazywany m.in. jako format dokumentów, raportów lub eksportów.
PDU	Power Distribution Unit – listwa lub jednostka dystrybucji zasilania, wykorzystywana w szafach RACK i infrastrukturze centrum danych.
PEL	Punkt elektryczno-logiczny – punkt instalacyjny obejmujący gniazda zasilające oraz punkty logiczne RJ45, stosowany w modernizowanej sieci teleinformatycznej.
PEM	Pole elektromagnetyczne. W PFU pojęcie występuje w kontekście oddziaływania instalacji radiowych, analiz radiowych, pozwoleń i wymagań środowiskowych.
PFU	Program Funkcjonalno-Użytkowy – podstawowy dokument opisujący przedmiot zamówienia realizowanego w formule „zaprojektuj i zbuduj”, wymagania Zamawiającego oraz informacje niezbędne do zaprojektowania i wykonania zamierzenia.
PGW Wody Polskie	Państwowe Gospodarstwo Wodne Wody Polskie – podmiot zarządzający gospodarką wodną oraz wieloma obiektami i terenami istotnymi dla lokalizacji infrastruktury RIS.
PKP PLK	PKP Polskie Linie Kolejowe S.A. – zarządca infrastruktury kolejowej, w tym mostów kolejowych, na których lub przy których mogą być lokalizowane elementy systemu RIS.

PoE	Power over Ethernet – technologia zasilania urządzeń przez kabel sieciowy Ethernet, stosowana m.in. dla punktów RJ45, kamer, tabletów informacyjnych lub urządzeń sieciowych.
PowerProtect DP4400	Nazwa handlowa rozwiązania Dell Technologies do ochrony danych, powiązanego z Dell EMC Avamar DP4400 / IDPA, wykorzystywanego przez Zamawiającego.
PTZ	Pan-Tilt-Zoom – funkcje kamery umożliwiające obrót w poziomie, pochylenie w pionie oraz zdalne przybliżenie obrazu.
Pzp / ustawa Pzp	Ustawa z dnia 11 września 2019 r. Prawo zamówień publicznych. Akt prawny regulujący zasady przygotowania i prowadzenia postępowania o udzielenie zamówienia publicznego.
QoS	Quality of Service – mechanizmy jakości usług w sieciach teleinformatycznych, umożliwiające priorytetyzację i kontrolę parametrów transmisji danych.
QUINT-UPS/1AC/1AC/500VA	Typ istniejącego lub referencyjnego zasilacza awaryjnego stosowanego w systemie RIS. W PFU nazwa występuje w kontekście wymiany lub dostawy równoważnych zasilaczy awaryjnych.
RACK	Standard montażu urządzeń teleinformatycznych w szafach technicznych, zwykle o szerokości 19 cali. W PFU pojęcie stosowane w odniesieniu do szaf serwerowych, telekomunikacyjnych i teletechnicznych.
RAID	Redundant Array of Independent Disks – mechanizm organizacji dysków zapewniający zwiększenie dostępności, wydajności lub ochrony danych.
RAM	Random Access Memory – pamięć operacyjna serwera lub urządzenia komputerowego. W PFU pojęcie występuje w wymaganiach dla zasobów obliczeniowych.
RJ45	Typ złącza stosowanego w okablowaniu strukturalnym Ethernet. W PFU pojawia się przy wymaganiach dotyczących punktów logicznych i modernizacji sieci teleinformatycznej.
RODO	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 dotyczące ochrony danych osobowych. W PFU pojęcie odnosi się do wymagań przetwarzania, ochrony i bezpieczeństwa danych osobowych.
RPO	Recovery Point Objective – maksymalny akceptowalny punkt utraty danych wyrażony czasem od ostatniej poprawnej kopii, repliki lub zapisu danych.
RS-232	Standard szeregowego interfejsu komunikacyjnego, stosowany w komunikacji z urządzeniami i sensorami.
RS-422	Standard szeregowego interfejsu komunikacyjnego umożliwiający transmisję różnicową, stosowany w komunikacji z urządzeniami i sensorami.
RS-485	Standard szeregowego interfejsu komunikacyjnego wykorzystywany m.in. w automatyce, pomiarach i komunikacji z czujnikami.
RSRP	Reference Signal Received Power – parametr mocy sygnału referencyjnego w sieciach LTE/5G, wykorzystywany do oceny jakości zasięgu w analizach transmisji komórkowej.

RSRQ	Reference Signal Received Quality – parametr jakości sygnału referencyjnego w sieciach LTE/5G, wykorzystywany do oceny jakości połączenia radiowego w analizach transmisji komórkowej.
RTCM	Radio Technical Commission for Maritime Services – standard transmisji poprawek różnicowych stosowany m.in. w systemach DGNSS/DGPS.
RTO	Recovery Time Objective – maksymalny akceptowalny czas przywrócenia działania usługi, systemu lub komponentu po awarii.
RTP	Real-time Transport Protocol – protokół transmisji danych czasu rzeczywistego, stosowany m.in. przy strumieniowaniu audio lub wideo.
RTU	Remote Terminal Unit albo Modbus RTU – w PFU pojęcie może występować w kontekście komunikacji z urządzeniami pomiarowymi, sensorami i lokalnymi komponentami akwizycji danych.
RZGW	Regionalny Zarząd Gospodarki Wodnej – jednostka organizacyjna PGW Wody Polskie zarządzająca wybranymi obiektami hydrotechnicznymi i terenami istotnymi dla systemu RIS.
SAN	Storage Area Network – dedykowana sieć dostępu do zasobów pamięci masowej, stosowana w środowiskach serwerowych i centrum danych.
SAT	Site Acceptance Tests – testy akceptacyjne wykonywane w miejscu instalacji lub eksploatacji rozwiązania, potwierdzające spełnienie wymagań po wdrożeniu.
SDI-12	Serial Digital Interface at 1200 baud – standard komunikacji z czujnikami środowiskowymi, wykorzystywany m.in. w hydrologii i meteorologii.
Sensor meteorologiczny	Urządzenie pomiarowe służące do pomiaru parametrów meteorologicznych, w szczególności prędkości i kierunku wiatru, temperatury, wilgotności, ciśnienia atmosferycznego oraz opadów.
Serwerownia główna	Podstawowe pomieszczenie lub środowisko techniczne Zamawiającego przeznaczone do utrzymywania centralnych zasobów serwerowych i sieciowych systemu RIS.
Serwerownia telekomunikacyjna	Modernizowane pomieszczenie pełniące funkcję węzła telekomunikacyjnego, koncentracji sieci LAN i elementów transmisyjnych, powiązane z ciągłością komunikacji lokalizacji RIS z systemem centralnym.
SFP / SFP+	Small Form-factor Pluggable – moduł transceivera stosowany w przełącznikach i urządzeniach sieciowych do realizacji połączeń światłowodowych lub miedzianych.
SH API	API Systemu Hydrologii IMGW-PIB, wykorzystywane do przekazywania danych pomiarowych z wodowskazów systemu RIS do systemu IMGW-PIB.
SLA	Service Level Agreement – parametry poziomu świadczenia usług, w szczególności czasy reakcji, czasy usunięcia awarii, dostępność, zasady raportowania i odpowiedzialność serwisowa.
SNMP	Simple Network Management Protocol – protokół zarządzania i monitorowania urządzeń sieciowych oraz infrastruktury teleinformatycznej.
SSD	Solid State Drive – półprzewodnikowy nośnik danych. W PFU pojęcie stosowane przy wymaganiach dotyczących macierzy dyskowych i rozbudowy pamięci masowej.

Stacja bazowa AIS	Brzegowa stacja systemu AIS zapewniająca odbiór, nadawanie, wymianę i przekazywanie danych AIS w ramach systemu RIS.
Stacja bazowa VHF	Brzegowa stacja radiokomunikacyjna VHF zapewniająca łączność głosową lub obsługę kanałów radiowych wymaganych dla systemu RIS.
Studium Wykonalności / SW	Dokument analityczny stanowiący podstawę przygotowania projektu, opisujący zakres, uzasadnienie, warianty, koszty, cele i uwarunkowania realizacji projektu.
SWZ	Specyfikacja Warunków Zamówienia – dokument postępowania o udzielenie zamówienia publicznego określający warunki udziału, opis przedmiotu zamówienia, kryteria oceny ofert, projektowane postanowienia umowy i inne wymagania formalne.
System RIS	Zintegrowany system usług informacji rzecznej obejmujący infrastrukturę terenową, sensory, transmisję danych, Centrum RIS, systemy operatorskie, usługi cyfrowe, integracje, dane i procedury eksploatacyjne.
Szafa RACK	Szafa techniczna lub serwerowa przeznaczona do montażu urządzeń w standardzie 19 cali, stosowana w serwerowniach, punktach koncentracji i ośrodkach przetwarzania danych.
Szafa teletechniczna	Szafa przeznaczona do instalacji urządzeń telekomunikacyjnych, transmisyjnych, zasilających, zabezpieczających i monitorujących. W PFU pojęcie dotyczy zwłaszcza szaf terenowych typu zewnętrznego.
TB	Terabajt – jednostka pojemności danych, stosowana m.in. przy określaniu pojemności macierzy, repozytoriów, kopii zapasowych i zasobów pamięci masowej.
TEN-T	Trans-European Transport Network – transeuropejska sieć transportowa. W PFU pojęcie występuje w kontekście znaczenia Odrzańskiej Drogi Wodnej i zgodności projektu z polityką transportową UE.
TLS	Transport Layer Security – protokół kryptograficzny zapewniający poufność i integralność transmisji danych, stosowany m.in. w usługach HTTPS, API i zdalnym dostępie administracyjnym.
Tor podstawowy	Podstawowy tor transmisji danych, zasilania lub komunikacji wykorzystywany w normalnym trybie pracy systemu.
Tor zapasowy	Rezerwowy tor transmisji danych, zasilania lub komunikacji uruchamiany w przypadku awarii, niedostępności albo degradacji toru podstawowego.
UKE	Urząd Komunikacji Elektronicznej – organ właściwy m.in. w sprawach częstotliwości, pozwoleń radiowych i radiokomunikacji.
UTM	Unified Threat Management – urządzenie lub rozwiązanie bezpieczeństwa łączące funkcje zapory sieciowej, VPN, filtrowania, ochrony przed zagrożeniami i monitorowania ruchu.
UPS	Uninterruptible Power Supply – zasilacz awaryjny zapewniający podtrzymanie zasilania urządzeń w przypadku zaniku lub zakłócenia zasilania podstawowego.
UPS-BAT/VRLA-WTR/24DC/13AH	Oznaczenie typu modułu bateryjnego stosowanego z zasilaczem QUINT-UPS/1AC/1AC/500VA albo rozwiązaniem równoważnym.
URL	Uniform Resource Locator – adres zasobu w sieci, np. adres usługi API, strony internetowej, dokumentacji lub endpointu integracyjnego.

Usługa Utrzymania	Usługa realizowana po wdrożeniu systemu RIS, obejmująca działania utrzymaniowe, monitorowanie, obsługę zgłoszeń, reagowanie na awarie, aktualizacje, wsparcie, raportowanie i inne czynności określone w PFU oraz Umowie.
UŻŚ	Urząd Żeglugi Śródlądowej – urząd administracji żeglugi śródlądowej. W PFU pojęcie odnosi się przede wszystkim do Zamawiającego, tj. Urzędu Żeglugi Śródlądowej w Szczecinie.
VEGAMET	Nazwa rodziny urządzeń wykorzystywanych w istniejącym systemie wodowskazowym, stosowana w PFU jako element opisu stanu istniejącego.
VEGAPULS	Nazwa rodziny radarowych czujników poziomu, wykorzystywanych w istniejącym systemie wodowskazowym, stosowana w PFU jako element opisu stanu istniejącego.
VHF	Very High Frequency – zakres fal radiowych od 30 MHz do 300 MHz. W PFU pojęcie dotyczy radiokomunikacji głosowej i infrastruktury łączności radiowej systemu RIS.
VHF/AIS	Łączne określenie infrastruktury radiokomunikacyjnej obejmującej łączność VHF oraz system AIS.
VHF/AIS/DGNSS	Łączne określenie infrastruktury radiokomunikacyjnej obejmującej łączność VHF, system AIS oraz funkcję DGNSS.
VLAN	Virtual Local Area Network – wirtualna sieć lokalna służąca do logicznej separacji ruchu w sieci LAN.
VMS	Video Management System – system zarządzania obrazem wideo, kamerami, rejestracją, podglądem i uprawnieniami w systemie CCTV.
VPN	Virtual Private Network – wirtualna sieć prywatna zapewniająca bezpieczne połączenie pomiędzy lokalizacjami lub systemami przez sieć publiczną albo operatorską.
VSS	Video Surveillance System – system dozoru wizyjnego, pojęcie stosowane zamiennie lub uzupełniająco względem CCTV w kontekście norm technicznych.
VTMS	Vessel Traffic Management Solution – rozwiązanie do zarządzania ruchem statków, powiązane funkcjonalnie z usługami śledzenia, prezentacji i analizy ruchu jednostek.
VTS	Vessel Traffic Service – służba kontroli ruchu statków. Pojęcie powiązane z zarządzaniem ruchem jednostek, choć RIS nie jest tożsame z morskim VTS.
VTT	Vessel Tracking and Tracing – usługa śledzenia i namierzania statków, obejmująca prezentację aktualnego ruchu jednostek, historię ruchu, wyszukiwanie, strefy, bramki, alarmy, ETA i statystyki.
WAN	Wide Area Network – sieć rozległa łącząca oddalone lokalizacje systemu RIS z Centrum RIS lub innymi ośrodkami.
WCAG	Web Content Accessibility Guidelines – wytyczne dostępności treści internetowych, stanowiące punkt odniesienia dla dostępności cyfrowej usług, aplikacji, dokumentów i interfejsów.

Wodowskaz	Urządzenie lub zestaw urządzeń służących do pomiaru poziomu wody, w szczególności z wykorzystaniem czujników radarowych i odniesień geodezyjnych.
WWW	World Wide Web – usługa internetowa lub środowisko stron internetowych, wykorzystywane w kontekście portali, usług cyfrowych i dostępu przez przeglądarkę.
XML	Extensible Markup Language – tekstowy format zapisu danych, stosowany w wymianie danych, konfiguracji lub dokumentacji technicznej.
XLS	Format pliku arkusza kalkulacyjnego Microsoft Excel starszego typu. W PFU może występować jako format eksportu raportów lub zestawień.
XLSX	Format pliku arkusza kalkulacyjnego Microsoft Excel nowszego typu, stosowany jako format eksportu raportów, zestawień lub danych.
Zamawiający	Urząd Żeglugi Śródlądowej w Szczecinie, działający jako podmiot zamawiający w postępowaniu dotyczącym rozbudowy systemu RIS na Odrzańskiej Drodze Wodnej.
Zasilacz awaryjny	Urządzenie UPS lub równoważne rozwiązanie zapewniające podtrzymanie zasilania urządzeń systemu RIS w przypadku zaniku albo pogorszenia parametrów zasilania podstawowego.
Źródła danych systemu RIS	Urządzenia, systemy i integracje dostarczające dane do systemu RIS, w szczególności AIS, VHF, CCTV, wodowskazy, sensory meteorologiczne, urządzenia transmisyjne, systemy monitoringu technicznego i systemy zewnętrzne.