

Opis Przedmiotu Zamówienia

System Informacji Przestrzennej Resortu Obrony Narodowej (SIPRON) oraz System Elektronicznych Usług (e-usługi).

Projekt e-infrastruktura MON finansowany ze środków pochodzących z Inwestycji C2.1.1 „E-usługi publiczne, rozwiązania IT usprawniające funkcjonowanie administracji i sektorów gospodarki” w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

1. Definicje i skróty

Pojęcie / skrót	Definicja
SIPRON	System Informacji Przestrzennej Resortu Obrony Narodowej – podstawowy system GIS będący przedmiotem licencjonowania i wdrożenia w ramach niniejszego zamówienia
e-usługi	Dedykowany system do elektronicznej obsługi wniosków i spraw kierowanych do MON przez podmioty zewnętrzne, ściśle współpracujący z SIPRON
GIS	Geographic Information System – system informacji geograficznej do wprowadzania, gromadzenia, przetwarzania i wizualizacji danych przestrzennych
Kubernetes (K8s)	Platforma do orkiestracji kontenerów, na której zostanie wdrożony SIPRON w architekturze rozproszonej na infrastrukturze Zamawiającego
PostGIS	Rozszerzenie bazy danych PostgreSQL umożliwiające przechowywanie i przetwarzanie danych przestrzennych – główna baza danych systemu SIPRON
WMS/WMTS/WFS	Standardy OGC do udostępniania danych przestrzennych w postaci map rastrowych (WMS/WMTS) i danych wektorowych (WFS) przez protokół HTTP
EZD/EOD	Elektroniczne Zarządzanie Dokumentami / Elektroniczny Obieg Dokumentów – system MON do zarządzania dokumentacją, z którym system e-usług musi się integrować
ePUAP/GOV.PL	Elektroniczna Platforma Usług Administracji Publicznej – kanał przyjmowania i przekazywania elektronicznych wniosków przez portal GOV.PL
API	Application Programming Interface – interfejs programistyczny do wymiany danych między systemami
QGIS	Darmowe oprogramowanie GIS używane przez pracowników MON do zaawansowanych analiz przestrzennych. System SIPRON musi zapewniać pełną interoperacyjność z QGIS

Pojęcie / skrót	Definicja
Rolling update	Procedura aktualizacji systemu bez przerwy w działaniu — kolejne pody Kubernetes są zastępowane nową wersją jeden po drugim
Disaster recovery	Procedura przywracania systemu do działania po katastrofalnej awarii na podstawie kopii zapasowych
SLA	Service Level Agreement — umowne czasy reakcji i usuwania błędów w ramach wsparcia i gwarancji
CVSS	Common Vulnerability Scoring System — standard oceny wagi podatności bezpieczeństwa (skala 0-10)
RODO	Rozporządzenie o Ochronie Danych Osobowych (GDPR) — wymagania w zakresie przetwarzania danych osobowych
DPIA	Data Protection Impact Assessment — ocena skutków dla ochrony danych, wymagana dla systemów wysokiego ryzyka
WCAG 2.1 AA	Web Content Accessibility Guidelines — standard dostępności cyfrowej wymagany dla portalu e-usług
OPZ	Opis Przedmiotu Zamówienia — niniejszy dokument

2. Kontekst i cel zamówienia

2.1. Kontekst organizacyjny

Ministerstwo Obrony Narodowej eksploatuje System Informacji Przestrzennej Resortu Obrony Narodowej (SIPRON). System funkcjonuje i spełnia oczekiwania Zamawiającego — jest używany przez pracowników MON do zarządzania danymi przestrzennymi związanymi z infrastrukturą i planowaniem resortu.

Niniejsze zamówienie obejmuje dwa ściśle powiązane obszary: kontynuację licencji na System SIPRON wraz z jego profesjonalnym wdrożeniem w architekturze Kubernetes na infrastrukturze MON, oraz stworzenie od podstaw systemu do obsługi elektronicznych usług (e-usług) kierowanych do resortu przez podmioty zewnętrzne. Oba systemy stanowią odrębne komponenty technicznie, jednak są ze sobą logicznie powiązane — pracownicy MON obsługujący wnioski e-usług będą korzystać z SIPRON jako narzędzia weryfikacji danych przestrzennych.

2.2. Cel zamówienia

Przedmiotem zamówienia jest kompleksowa usługa obejmująca:

1. dostarczenie licencji na System SIPRON zapewniających ciągłość działania systemu na warunkach zgodnych z jego dotychczasowym użytkowaniem,
2. wdrożenie SIPRON w architekturze opartej na Kubernetes na infrastrukturze serwerowej Zamawiającego, wraz z migracją danych i konfiguracją,
3. zaprojektowanie i wykonanie systemu do obsługi e-usług, zintegrowanego z SIPRON, systemem EZD/EOD Zamawiającego oraz platformą ePUAP/GOV.PL,
4. przeprowadzenie szkoleń dla użytkowników i administratorów,

5. dostarczenie kompletnej dokumentacji technicznej i użytkownika,
6. objęcie systemów gwarancją i asystą techniczną po wdrożeniu.

Uwaga dotycząca SIPRON

Zamawiający użytkuje SIPRON i jest z niego zadowolony. Niniejszy OPZ nie opisuje wymagań funkcjonalnych SIPRON od nowa — są one zawarte w Załączniku nr 1 (Wymagania funkcjonalne i нефункционалне systemu).

Zadaniem Wykonawcy jest dostarczenie licencji zapewniających ciągłość użytkowania oraz profesjonalne wdrożenie systemu w nowej architekturze Kubernetes z pełną dokumentacją i szkoleniami.

3. System e-usług — zakres i wymagania

3.1. Opis systemu e-usług

System e-usług stanowi nowe narzędzie do obsługi wniosków składanych drogą elektroniczną przez podmioty zewnętrzne (firmy, inwestorzy, instytucje publiczne, obywatele) do Ministerstwa Obrony Narodowej w sprawach wymagających uzgodnienia lub opinii MON. System umożliwia przygotowanie wniosku w przeglądarce, podpisanie go podpisem elektronicznym, opłacenie wymaganej opłaty oraz przekazanie do właściwego odbiorcy w MON z automatyczną rejestracją w systemie EZD/EOD.

3.2. Zakres e-usług objętych wdrożeniem

Wymaga się wdrożenia obsługi poniższych e-usług na 4. poziomie dojrzałości (formularz + pełny proces + obsługa sprawy):

Lp	Nazwa e-usługi	Uwagi
1	Zgłaszanie lokalizacji przeszkód lotniczych oraz wnioski o zaopiniowanie lokalizacji obiektu	Wymagana warstwa GIS ze strefami lotniczymi z SIPRON
2	Zgłaszanie lokalizacji lądowych farm wiatrowych	
3	Uzgadnianie decyzji o warunkach zabudowy	
4	Udostępnianie nieruchomości wojskowych	Wymagana weryfikacja lokalizacji względem mapy nieruchomości MON w SIPRON
5	Uzgadnianie lokalizacji lądowych farm fotowoltaicznych	
6	Uzgadnianie zezwolenia realizacji inwestycji drogowych	
7	Uzgadnianie decyzji o ustaleniu lokalizacji inwestycji celu publicznego	

Lp	Nazwa e-usługi	Uwagi
8	Wnioski do MPZP oraz studium uwarunkowań i kierunków zagospodarowania przestrzennego	
9	Opiniowanie budowy farm wiatrowych i zespołów urządzeń w polskich obszarach morskich	Możliwe wymogi specyficzne dotyczące obszarów morskich

3.3. Wymagania minimalne dla każdej e-usługi

Dla każdej z powyższych e-usług wymagane jest zapewnienie co najmniej:

- wypełnienia formularza w przeglądarce bez dodatkowego oprogramowania, z walidacją po stronie klienta i serwera,
- zapisu wersji roboczej wniosku i możliwości kontynuacji w późniejszym czasie,
- dołączania załączników (limity rozmiarów i dopuszczalnych formatów konfigurowalne przez administratora),
- podpisu elektronicznego — co najmniej: podpis zaufany (profil zaufany ePUAP) i podpis kwalifikowany,
- obsługi płatności online (jeśli opłata dotyczy danej usługi) z integracją z operatorem płatności,
- wysyłania wniosku do właściwego odbiorcy (routing) i automatycznej rejestracji w EZD/EOD,
- rejestracji sprawy i nadania numeru identyfikacyjnego,
- statusowania sprawy i komunikacji w toku (wezwania do uzupełnień, dosyłanie dokumentów),
- elektronicznego doręczenia odpowiedzi/rozstrzygnięcia.

3.4. Wymagania funkcjonalne systemu e-usług

3.4.1. Portal i katalog usług

- Katalog usług z wyszukiwarką i filtrowaniem po kategorii, rodzaju podmiotu, słowach kluczowych.
- Karta każdej usługi zawierająca: opis, wymagane załączniki, opłaty, czas realizacji, instrukcje, FAQ.
- Wersja mobilna (responsywny interfejs RWD) dla wszystkich ekranów procesu składania wniosku.
- Zgodność z WCAG 2.1 AA dla całego portalu i wszystkich ekranów procesu wnioskowego.

3.4.2. Panel użytkownika (wnioskodawcy)

- Panel użytkownika z listą złożonych wniosków, statusami, historią i dokumentami.
- Podgląd złożonych wniosków i dołączonych załączników.
- Widoczne potwierdzenia: złożenia wniosku, płatności, doręczenia.
- Powiadomienia e-mail o zmianie statusu, wezwaniach do uzupełnień, rozstrzygnięciach.

3.4.3. Formularze i podpis

- Dynamiczne formularze z walidacją realizowane jako kreator krokowy (wizard).
- Generator podglądu dokumentu PDF przed podpisem.
- Komponent lokalizacji (mapa GIS) — możliwość wskazania punktu na mapie, wprowadzenia współrzędnych, zapisu geometrii jako metadanych wniosku, eksportu do GeoJSON/WKT.
- Alternatywna, dostępna ścieżka wprowadzania lokalizacji (co najmniej adres lub współrzędne tekstowo) jako element dostępności WCAG.
- Walidacja podpisu i zapis wyniku walidacji przy sprawie.

3.4.4. Płatności i routing

- Integracja z operatorem płatności. Powiązanie transakcji z wnioskiem (ID, kwota, status, data).
- Obsługa statusów: opłacona / nieopłacona / odrzucona / przerwana. Możliwość ponowienia płatności.
- Elektroniczne przekazanie wniosku do właściwego odbiorcy — konfigurowalny routing na podstawie rodzaju usługi i wskazanej lokalizacji.
- Automatyczna rejestracja sprawy i dokumentów w systemie EZD/EOD Zamawiającego poprzez API.

3.4.5. Wymagania techniczne i kompatybilność

- Portal musi działać poprawnie w aktualnych stabilnych wersjach przeglądarek i w wersjach N-2: Google Chrome, Microsoft Edge (Chromium), Mozilla Firefox, Safari.
- Portal musi działać bez instalacji dodatkowych wtyczek, z wyjątkiem komponentu podpisu kwalifikowanego wymagającego aplikacji zewnętrznej dostawcy.
- Integracja z usługami GIS SIPRON (WMS/WFS) w zakresie komponentu mapowego formularzy e-usług.

4. Wdrożenie systemu

Wdrożenie obejmuje oba komponenty — SIPRON oraz system e-usług — i składa się z etapów: analiza przedwdrożeniowa, instalacja i konfiguracja, integracja, testowanie, odbiory, szkolenia i uruchomienie produkcyjne. Dokładny harmonogram zostanie określony w dokumencie analizy przedwdrożeniowej.

4.1. Analiza przedwdrożeniowa

Przed przystąpieniem do jakichkolwiek prac instalacyjno-konfiguracyjnych Wykonawca przeprowadzi analizę przedwdrożeniową trwającą nie krócej niż 4 tygodnie, zakończoną dokumentem zaakceptowanym przez Zamawiającego. Analiza przedwdrożeniowa jest formalnym warunkiem przystąpienia do kolejnego etapu.

Dokument analizy przedwdrożeniowej musi obejmować co najmniej:

1. projekt architektury technicznej klastra Kubernetes — dobór węzłów, wersje komponentów, schemat sieci i polityki sieciowe,

2. szczegółowy harmonogram prac z kamieniami milowymi i kryteriami akceptacji każdego etapu,
3. definicje scenariuszy testów akceptacyjnych (UAT) uzgodnionych z Zamawiającym,
4. zakres i format danych przeznaczonych do importu oraz plan migracji danych historycznych,
5. schematy integracji z systemami zewnętrznymi (EZD/EOD, ePUAP, operator płatności, operator podpisu),
6. ocenę ryzyk projektowych wraz z planem mitygacji,
7. listę oprogramowania open source używanego w systemie wraz z licencjami.

4.2. Instalacja systemu SIPRON w architekturze Kubernetes

System SIPRON zostanie wdrożony w architekturze mikrousług na klastrze Kubernetes zainstalowanym na infrastrukturze serwerowej Zamawiającego. Architektura musi zapewnić wysoką dostępność, możliwość skalowania i łatwość utrzymania przez wewnętrzny dział IT MON.

4.2.1. Architektura klastra

1. Klaster Kubernetes będzie składał się co najmniej z: trzech węzłów roboczych (worker nodes) gwarantujących dostępność przy awarii jednego węzła, planów sterowania (control plane) w konfiguracji HA, dedykowanej trwałej przestrzeni dyskowej (Persistent Volumes) dla bazy PostGIS, plików użytkowników i danych rastrowych, oraz lokalnego rejestru obrazów kontenerów (Container Registry).
2. Wykonawca wdroży co najmniej następujące składniki jako osobne Deployments/StatefulSets: aplikacja webowa SIPRON (frontend i backend API), baza danych PostGIS (PostgreSQL z rozszerzeniem PostGIS, w konfiguracji z replikacją), serwer mapowy (GeoServer lub równoważny) do obsługi WMS/WMTS/WFS, serwer plików (object storage) do przechowywania załączników i danych rastrowych, komponent systemu e-usług (frontend, backend, baza danych), reverse proxy/Ingress Controller z TLS, system zarządzania certyfikatami (cert-manager lub równoważny).
3. Cała konfiguracją klastra (manifesty YAML, Helm charts lub równoważne) musi być przechowywana w repozytorium kodu (git) i przekazana Zamawiającemu w ramach dokumentacji. Zamawiający musi być w stanie odtworzyć środowisko na podstawie dostarczonej dokumentacji bez udziału Wykonawcy.

4.2.2. Wysoka dostępność i skalowanie

1. Co najmniej 2 repliki dla każdej krytycznej usługi (frontend, backend API, serwer mapowy).
2. HorizontalPodAutoscaler (HPA) dla składników o zmiennym obciążeniu.
3. PodDisruptionBudget zapewniający dostępność co najmniej jednej repliki podczas planowych aktualizacji.
4. Readiness i liveness probes dla wszystkich kontenerów — automatyczne wykrywanie awarii i restart.

4.2.3. Sieć i izolacja

1. Polityki sieciowe (NetworkPolicy) zapewniające, że baza danych PostGIS jest dostępna wyłącznie dla aplikacyjnych składników SIPRON — bez bezpośredniego dostępu z zewnątrz.

2. Ruch zewnętrzny kierowany wyłącznie przez Ingress Controller na porcie 443 (HTTPS). Portal e-usług dostępny publicznie przez odrębny Ingress z Web Application Firewall (WAF).
3. SIPRON (część wewnętrzna) dostępny wyłącznie z sieci wewnętrznej MON.
4. Wykonawca dostarczy diagram architektury sieciowej z opisem kierunków ruchu.

4.2.4. Monitoring i observability

1. System zbierania metryk (np. Prometheus) z eksporterami dla węzłów Kubernetes, PostGIS i serwera mapowego.
2. Wizualizacja metryk i alarmowanie (np. Grafana) z predefiniowanymi dashboardami dla: zużycia CPU/RAM przez pody, dostępności usług, czasu odpowiedzi API, wielkości bazy danych.
3. Centralna agregacja logów (np. Loki lub ELK) zbierająca logi ze wszystkich podów.
4. Alerty powiadamiające administratora o krytycznych zdarzeniach: pod w stanie CrashLoopBackOff, brak miejsca na dysku, dostępność usługi poniżej 99%.

4.2.5. Kopie zapasowe i disaster recovery

1. Codzienny dump bazy danych PostGIS z retencją minimum 30 dni.
2. Replikacja Persistent Volumes zawierających dane użytkowników i dane rastrowe.
3. Backup konfiguracji klastra Kubernetes (eksport zasobów YAML lub stan etcd).
4. Kopie zapasowe muszą być składowane w lokalizacji fizycznie odrębnej od klastra produkcyjnego.
5. Przed odbiorem systemu Wykonawca przeprowadzi co najmniej jeden disaster recovery drill — pełną procedurę przywracania środowiska z kopii zapasowej, udokumentowaną protokołem.

4.2.6. Aktualizacje

1. Wykonawca zaprojektuje i udokumentuje procedurę aktualizacji bez przerwy w działaniu (rolling update): aktualizacja obrazów kontenerów, migracje schematu bazy z możliwością rollback, aktualizacja wersji Kubernetes.

4.3. Konfiguracja systemu SIPRON

1. Konfiguracja podstawowa: połączenie z bazą PostGIS, parametry puli połączeń, konfiguracją serwera mapowego (workspace, store, reguły publikacji WMS/WMTS/WFS), serwer poczty wychodzącej (SMTP), parametry bezpieczeństwa sesji, logo i identyfikacja wizualna Zamawiającego, układy współrzędnych (EPSG:2178, EPSG:4326, EPSG:3857).
2. Konfiguracja kont i uprawnień: role systemowe (administrator, redaktor danych, użytkownik przeglądający) z zestawami uprawnień, konta użytkowników według listy przekazanej przez Zamawiającego, ograniczenia przestrzenne (geofencing) dla użytkowników z dostępem tylko do wybranych obszarów, 2FA dla kont administratorskich.
3. Import danych przestrzennych: import warstw wektorowych (Shapefile, GeoJSON, GeoPackage) do bazy PostGIS z weryfikacją geometrii, konfiguracją symbolizacji warstw, import danych rastrowych (ortofotomapy, mapy archiwalne) do serwera mapowego, konfiguracją publikacji WMS/WMTS, import danych słownikowych.
4. Konfiguracja przestrzeni roboczych: kompozycje mapowe dla głównych przypadków użycia, domyślne warstwy podkładowe (ortofotomapa, mapa topograficzna), portale

publiczne na potrzeby e-usług z warstwami niezbędnymi do składania wniosków (strefy lotnicze, nieruchomości wojskowe, działki ewidencyjne).

4.4. Konfiguracja systemu e-usług

1. Formularze dla każdej z 9 e-usług wymienionych w pkt 3.2 – pola, walidacje, załączniki, zależności między polami.
2. Integracje z dostawcami zewnętrznymi: operator podpisu (ePUAP/profil zaufany, podpis kwalifikowany), operator płatności, routing wniosków do właściwych jednostek MON.
3. Szablony powiadomień e-mail dla wnioskodawców (potwierdzenie złożenia, wezwanie do uzupełnień, decyzja).
4. Integracja z systemem EZD/EOD poprzez API – automatyczna rejestracja wniosków i dokumentów.
5. Integracja komponentu GIS (mapy, warstwy z SIPRON) w formularzach e-usług.

4.5. Integracja z systemami zewnętrznymi

Wykonawca przeprowadzi analizę przedwdrożeniową integracji, zaprojektuje i wykona integracje w maksymalnym możliwym zakresie technicznym i budżetowym, oraz udokumentuje przyjęte rozwiązania i ich ograniczenia.

System	Kierunek integracji	Zakres
EZD/EOD (MON)	e-usługi EZD/EOD →	Automatyczna rejestracja wniosków i załączników, przekazywanie statusów, odbiór odpowiedzi/decyzji do e-usług
ePUAP / GOV.PL	e-usługi ePUAP →	Uwierzytelnianie wnioskodawców profilem zaufanym, podpis zaufany, przekazywanie wniosków przez skrzynkę ePUAP
Operator płatności	e-usługi operator →	Inicjowanie transakcji, odbiór potwierdzenia płatności, obsługa statusów i ponowień
QGIS	SIPRON ↔ QGIS	Połączenie przez WMS/WFS/WFS-T lub dedykowaną wtyczkę; edycja danych z QGIS z zapisem w PostGIS
Usługi GUGiK (WMS/WMTS)	zewnętrzne SIPRON →	Wczytanie podkładów mapowych (ortofotomapa, BDOT10k, ULDK dla wyszukiwania działek)

4.6. Testowanie

Wykonawca wspólnie z Zamawiającym wykona testy akceptacyjne (UAT) na podstawie scenariuszy testowych opracowanych w fazie analizy przedwdrożeniowej. Scenariusze będą zawierać testy funkcjonalne, wydajnościowe (100–500 użytkowników SIPRON jednocześnie) oraz testy bezpieczeństwa. Pozytywne przejście testów jest warunkiem podpisania protokołu odbioru.

Wykonawca przeprowadzi i udokumentuje testy bezpieczeństwa przed odbiorem: statyczną analizę kodu (SAST), skanowanie podatności zależności (SCA) oraz test penetracyjny aplikacji webowych (DAST) zgodny z OWASP Top 10. Raport z testów i dowody usunięcia krytycznych podatności zostaną przekazane Zamawiającemu.

4.7. Dokumentacja

Wykonawca dostarczy kompletną dokumentację obejmującą:

Dokument	Odbiorca	Format	Zawartosc minimalna
Dokumentacja użytkownika SIPRON	Użytkownicy końcowi	PDF (dostępny z poziomu aplikacji)	Opis wszystkich funkcji, zrzuty ekranu, przykładowe scenariusze użycia
Dokumentacja użytkownika e-usług – panel wnioskodawcy	Wnioskodawcy zewnętrzni	HTML/PDF w portalu	Instrukcja składania wniosku krok po kroku dla każdej z 9 e-usług
Dokumentacja operatora e-usług	Pracownicy MON obsługujący sprawy	PDF	Instrukcja obsługi panelu spraw, integracja z EZD/EOD
Dokumentacja administratora SIPRON	Administratorzy aplikacji MON	PDF	Zarządzanie użytkownikami, import danych, konfiguracją warstw, portale publiczne
Dokumentacja administratora IT (Kubernetes)	Dział IT MON	PDF + repo git	Architektura klastra, procedury start/stop/restart, monitoring, aktualizacje, backup/restore, disaster recovery
Dokumentacja deweloperska	MON / ewentualni przyszli wykonawcy	PDF + repo git	Opis API, schemat bazy danych, instrukcja budowania obrazów, opis zmiennych konfiguracyjnych

5. Szkolenia

Wykonawca przeprowadzi szkolenia dla pracowników Zamawiającego umożliwiające samodzielną pracę na wdrożonym systemie. Harmonogram szkoleń zostanie uzgodniony podczas analizy przedwdrożeniowej. Szkolenia muszą zostać przeprowadzone przed uruchomieniem systemu produkcyjnego.

Bl ok	Nazwa	Czas	Uczestnicy	Zakres
1	Użytkownicy SIPRON – obsługa systemu GIS	8h (1 dzień)	Pracownicy MON korzystający z SIPRON, ~100 os.	Logowanie i zarządzanie sesją, przeglądanie danych na mapie, obsługa warstw i symbolizacji, narzędzia pomiarowe, wydruki, edycja danych przestrzennych (dla uprawnionych), moduł dokumentów, moduł zadań, obsługa aplikacji

Bl ok	Nazwa	Czas	Uczestnicy	Zakres
				mobilnej. Ćwiczenia praktyczne na danych testowych.
2	Administratorzy SIPRON – administracja aplikacją	16h (2 dni)	(2 Administratorzy systemu po stronie MON, ~3–5 os.	Zarządzanie kontami i uprawnieniami, import i zarządzanie warstwami GIS, konfiguracją symbolizacji, zarządzanie słownikami, tworzenie i konfiguracją portali publicznych, konfiguracją serwera mapowego, monitoring aplikacji z poziomu paneli administracyjnych, procedury kopii zapasowych.
3	Administratorzy IT – infrastrukturą Kubernetes	16h (2 dni)	(2 Administratorzy IT MON odpowiedzialni za klaster, ~3–5 os.	Architektura klastra Kubernetes, obsługa kubectl i pulpitów zarządzania, procedury start/stop/restart usług, monitorowanie stanów podów i węzłów (Prometheus/Grafana), analiza logów, rolling update, tworzenie i weryfikacja kopii zapasowych PostGIS, disaster recovery, zarządzanie certyfikatami TLS. Wymaga wiedzy z zakresu Linux i sieci.
4	Operatorzy e-usług – obsługa wniosków po stronie MON	4h (pół dnia)	(Pracownicy MON obsługujący wpływające wnioski, ~20–30 os.	Panel obsługi spraw, przegląd i weryfikacja złożonych wniosków, statusowanie i komunikacja z wnioskodawcą, wezwania do uzupełnień, obsługa załączników i podpisów elektronicznych, routing spraw do właściwych jednostek, integracja z EZD/EOD, generowanie potwierdzeń.

Szkolenia będą prowadzone stacjonarnie w siedzibie Zamawiającego lub w formie zdalnej (webinar) — do uzgodnienia podczas analizy przedwdrożeniowej. Wykonawca zapewni materiały szkoleniowe w wersji elektronicznej (PDF) dla wszystkich uczestników.

6. Bezpieczeństwo IT

6.1. Wymagania dotyczące transmisji i uwierzytelniania

1. Cała transmisja danych między klientem a serwerem musi być szyfrowana z użyciem TLS w wersji co najmniej 1.2 (rekomendowane 1.3). Certyfikaty muszą być wydane przez uznany urząd certyfikacji lub infrastrukturę PKI Zamawiającego.
2. System musi posiadać mechanizm wykrywania i blokowania wielokrotnych nieudanych prób logowania (brute-force protection). Po przekroczeniu konfigurowalnego progu konto zostaje tymczasowo zablokowane, a administrator otrzymuje powiadomienie.
3. Hasła użytkowników muszą być przechowywane wyłącznie w postaci haszowanej z użyciem algorytmu bcrypt lub Argon2. Przechowywanie haseł w postaci jawnej jest bezwzględnie niedopuszczalne.
4. Błędy uwierzytelniania nie mogą ujawniać informacji o tym, czy konto istnieje w systemie (unikanie enumeracji kont).

6.2. Architektura bezpieczeństwa

1. Część SIPRON działająca w sieci wewnętrznej MON musi być niedostępna z publicznego Internetu. Oddzielenie sieci wewnętrznej od publicznej musi być zrealizowane na poziomie konfiguracji sieciowej klastra (NetworkPolicy) i firewalla infrastrukturalnego.
2. Dostęp do portalu e-usług (publicznie dostępnego) musi być realizowany przez odrębny punkt wejściowy (Ingress) z zastosowaniem Web Application Firewall (WAF) lub równoważnego mechanizmu ochrony przed atakami OWASP Top 10.
3. Baza danych PostGIS oraz serwer plików muszą być dostępne wyłącznie dla aplikacyjnych składników systemu — bez bezpośredniego dostępu sieciowego z zewnątrz.
4. Wykonawca skonfiguruje polityki bezpieczeństwa nagłówków HTTP dla obu komponentów dostępnych przez przeglądarkę: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security (HSTS), X-Content-Type-Options, Referrer-Policy.

6.3. Testy bezpieczeństwa

1. Wykonawca przeprowadzi testy bezpieczeństwa przed odbiorem systemu obejmujące: statyczną analizę kodu źródłowego (SAST), skanowanie podatności zależności i bibliotek zewnętrznych (SCA), dynamiczny test penetracyjny aplikacji webowych (DAST) obejmujący co najmniej OWASP Top 10 dla obu komponentów (SIPRON i e-usługi).
2. Raport z testów bezpieczeństwa musi zostać przekazany Zamawiającemu wraz z opisem znalezionych podatności, ich klasyfikacją (CVSS) i dowodem ich usunięcia lub akceptowanego ryzyka resztkowego przed odbiorem końcowym.
3. Podatności o ocenie CVSS ≥ 7.0 muszą zostać usunięte przed odbiorem. Wyjątki wymagają pisemnej zgody Zamawiającego z udokumentowanym uzasadnieniem i planem mitygacji.

6.4. Ochrona danych osobowych

1. System musi spełniać wymagania RODO w zakresie przetwarzania danych osobowych. Szczególną uwagę należy przykładąć do systemu e-usług, który przetwarza dane wnioskodawców (osoby fizyczne i reprezentanci podmiotów).
2. Wykonawca dostarczy dokumentację DPIA (Data Protection Impact Assessment) dla komponentu e-usług przed jego wdrożeniem produkcyjnym.
3. System musi zapewniać możliwość realizacji praw podmiotów danych: wglądu, sprostowania i usunięcia danych osobowych w zakresie wynikającym z przepisów.

6.5. Monitoring bezpieczeństwa i logi audytowe

1. System musi rejestrować następujące zdarzenia w logu audytowym: logowania udane i nieudane (z adresem IP), wszelkie modyfikacje danych przestrzennych, tworzenie, edycje i usuwanie kont użytkowników, eksport danych, zmiany konfiguracji systemu.
2. Logi audytowe muszą zawierać: identyfikator użytkownika, datę i godzinę (UTC), typ operacji, identyfikator obiektu lub zasobu, adres IP klienta.
3. Logi audytowe muszą być chronione przed modyfikacją przez użytkowników systemu i przechowywane przez co najmniej 12 miesięcy.
4. System musi mieć skonfigurowane regularne backupy z interwałem uzgodnionym z Zamawiającym, kopie lokalne (NAS lub równoważne) oraz ochronę przed utratą danych (RAID dla warstwy przechowywania).

7. Gwarancja

1. Wykonawca udzieli gwarancji na poprawne działanie całego Systemu (SIPRON oraz system e-usług) na okres 5 lat liczonych od daty podpisania bezwarunkowego protokołu odbioru końcowego.
2. Gwarancja obejmuje: naprawę błędów oprogramowania rozumianych jako niezgodności działania systemu z dostarczoną dokumentacją, dostarczanie aktualizacji bezpieczeństwa eliminujących podatności o ocenie CVSS ≥ 7.0 w terminie nie dłuższym niż 14 dni od opublikowania łatki przez producenta, utrzymanie zgodności z aktualnymi wersjami LTS/LTR używanych komponentów open source.
3. Gwarancja nie obejmuje: awarii wynikających z nieprawidłowej obsługi lub konfiguracji systemu przez personel Zamawiającego, udokumentowanej w logach systemowych; modyfikacji kodu lub konfiguracji dokonanych przez Zamawiającego bez pisemnej zgody Wykonawcy; awarii sprzętu leżących po stronie Zamawiającego; działań sił wyższych.
4. Casy reakcji i usunięcia wad w ramach gwarancji są tożsame z czasami wsparcia określonymi w rozdziale 8.
5. W przypadku stwierdzenia wady Wykonawca potwierdzi przyjęcie zgłoszenia gwarancyjnego w terminie 4 godzin roboczych od przekazania.
6. Zamawiający ma prawo żądać przekazania kodu źródłowego systemu wraz z pełną dokumentacją deweloperską i instrukcją budowania środowiska w przypadku: ogłoszenia upadłości lub likwidacji Wykonawcy; niewywiązywania się z obowiązków gwarancyjnych przez okres dłuższy niż 30 dni; rozwiązania umowy z przyczyn leżących po stronie Wykonawcy. Kod źródłowy przekazany w takim przypadku objęty jest licencją umożliwiającą Zamawiającemu utrzymanie i modyfikacje systemu na własne potrzeby.

8. Wsparcie techniczne

8.1. Okres i warunki wsparcia

1. Wykonawca udzieli wsparcia technicznego przez okres 24 miesięcy od daty podpisania protokołu odbioru.

2. Wykonawca udostępni dedykowany system ticketowy do rejestrowania zgłoszeń. Każde zgłoszenie otrzyma unikalny numer identyfikacyjny i automatyczne potwierdzenie przyjęcia e-mailem. Zamawiający będzie mógł śledzić status zgłoszeń w systemie ticketowym.
3. Wykonawca udostępni Zamawiającemu dedykowaną osobę do obsługi wsparcia oraz adres e-mail i numer telefonu do kontaktu w sprawach pilnych.
4. Godziny świadczenia wsparcia: poniedziałek–piątek, godz. 8:00–17:00, z wyjątkiem dni ustawowo wolnych od pracy. Dla błędów krytycznych – dostępność całodobowa przez 7 dni w tygodniu.

8.2. Czasy reakcji i usunięcia błędów

Kategoria błędu	Definicja	Czas reakcji	Czas usunięcia
Krytyczny	System całkowicie niedostępny lub moduły rozliczeń/e-usług nie działają uniemożliwiając przyjmowanie wniosków	2 godziny (7x24)	12 godzin od zgłoszenia
Poważny	Użytkownicy mają dostęp, ale nie mogą wykonać ważnej czynności (edycja, eksport, podpisywanie, płatność)	4 godziny robocze	48 godzin od zgłoszenia
Pomniejszy	Błędy nieistotnie wpływające na pracę użytkowników, niedogodności estetyczne lub brakujące funkcje niebędące częścią odbioru	1 dzień roboczy	5 dni roboczych od zgłoszenia

8.3. Zakres wsparcia

1. Wsparcie obejmuje: konsultacje w zakresie obsługi i konfiguracji systemu, pomoc w interpretacji logów systemowych, doradztwo w zakresie importu i zarządzania danymi przestrzennymi, wsparcie przy integracjach z systemami zewnętrznymi (EZD/EOD, ePUAP) w zakresie interfejsów dostarczonych przez Wykonawcę.
2. Wykonawca zobowiązuje się do dostarczania poprawek (patchy) obejmujących: aktualizacje bezpieczeństwa komponentów, poprawki błędów zgłoszonych przez Zamawiającego, aktualizacje wynikające ze zmian w zewnętrznych API (ePUAP, EZD, usługi GUGiK) w zakresie niezbędnym do zachowania ciągłości działania.
3. W ramach wsparcia Wykonawca przeprowadzi co najmniej jeden roczny przegląd techniczny systemu (health check) obejmujący: analizę logów pod kątem anomalii i błędów, ocenę wydajności i zajętości zasobów klastra, ocenę aktualności komponentów z rekomendacjami aktualizacji, weryfikację poprawności działania kopii zapasowych. Wynik zostanie przekazany w formie pisemnego raportu.
4. Na 3 miesiące przed upływem okresu wsparcia Wykonawca zaproponuje warunki przedłużenia lub prześle Zamawiającemu kompletną dokumentację umożliwiającą przekazanie systemu innemu podmiotowi.

Załącznik nr 1 — Wymagania funkcjonalne i нефункционаłne systemu SIPRON

Załącznik nr 1 zawiera szczegółowy opis wymagań funkcjonalnych i нефункционаłnych systemu SIPRON. Wymagania te odzwierciedlają aktualną funkcjonalność systemu użytkowanego przez Zamawiającego i stanowią podstawę do oceny oferty w zakresie dostarczenia licencji. Wykaz wymagań obejmuje następujące obszary:

- Wymagania нефункционаłne (język, system operacyjny, licencję, layout, bezpieczeństwo, skalowalność).
- Wymagania funkcjonalne — część dostępna przez przeglądarkę: zarządzanie danymi przestrzennymi, zarządzanie użytkownikami, funkcjonalności mapowe, edycja danych przestrzennych, serwer mapowy danych rastrowych, administracja systemem, moduł generowania portali publicznych, moduł dokumentów, moduł planowania i rozliczania zadań, moduł zadań, moduł raportów, inne (geokoder, wyszukiwarka działek, wyszukiwarka obiektów, zakładki przestrzenne).
- Wymagania wtyczki do QGIS.
- Funkcjonalności branżowe.

Uwaga

Pełna treść Załącznika nr 1 z ponumerowanymi wymaganiami stanowi odrębny dokument przekazywany Wykonawcom jako część dokumentacji przetargowej.

Wykonawca zobowiązany jest do potwierdzenia spełnienia każdego wymagania oznaczonego jako obowiązkowe w Załączniku nr 1.