Załącznik nr 1
SIWZ

Załącznik nr 1
do umowy ……. z dnia …….

Szczegółowy Opis Przedmiotu Zamówienia

Warunki realizacji zamówienia

na

Usługi konfiguracji i konserwacji urządzeń teleinformatycznych w centrach zarządzających i na stacjach referencyjnych systemu ASG-EUPOS

Spis treści

1. Słownik

Tabela 1. Słownik

Pojęcie/ Skrót	Opis
Administrator	Pracownik Zamawiającego nadzorujący pracę sprzętu teleinformatycznego i oprogramowania w centrum zarządzającym ASG-EUPOS
Audyt informatyczny	Sprawdzenie i zarchiwizowanie konfiguracji systemu przez Wykonawcę przed rozpoczęciem usług wsparcia informatycznego
Centrum zarządzające	Pomieszczenia, sprzęt teleinformatyczny, oprogramowanie i wyposażenie wykorzystywane na potrzeby systemu ASG-EUPOS
Czas reakcji	Czas w godzinach lub dniach, liczony od momentu pozyskania przez Wykonawcę informacji o incydencie do powiadomienia Zamawiającego o sposobie i terminie rozwiązania incydentu
Czas obsługi	Czas w godzinach lub dniach, liczony od momentu pozyskania przez Wykonawcę informacji o incydencie do momentu przekazania, przez Wykonawcę informacji o rozwiązaniu incydentu
Dokumentacja	Wszelkie dokumenty, oprogramowanie lub procedury powstałe w związku z realizacja zamówienia.
Dokumentacja powykonawcza	Dokumentacja systemu ASG-EUPOS obejmująca: projekt funkcjonalny, dokumentację techniczną i powykonawczą systemu, instrukcje użytkowania i procedury bezpieczeństwa informacji
Godzina wsparcia	Okres czasu trwający godzinę zegarową poświęcony przez Wykonawcę na wsparcie informatyczne świadczone bezpośrednio lub zdalnie.
Godziny pracy	Od 8:00 do 15:00 z wyłączeniem dni ustawowo wolnych od pracy, przy czym sobota jest traktowana jako dzień wolny od pracy
Incydent krytyczny	Usterka lub awaria uniemożliwiająca korzystanie z jednej lub wszystkich usług systemu ASG-EUPOS
Incydent pilny	Usterka lub awaria powodująca obniżenie jakości jednej lub wszystkich usług systemu ASG-EUPOS
Incydent standardowy	Każda awaria lub usterka sprzętu informatycznego lub oprogramowania
Oprogramowanie	Oprogramowanie systemowe i aplikacyjne (użytkowe) stosowane w centrum zarządzającym oraz na stacjach referencyjnych systemu ASG-EUPOS
Podmiot trzeci	Przedsiębiorca, instytucja lub osoba fizyczna wykonująca usługi na rzecz systemu ASG-EUPOS
Portal PZGiK	Portal internetowy obsługujący wnioski użytkowników systemu ASG-EUPOS
Praca zdalna	Wykonywanie usług informatycznych spoza centrum zarządzającego ASG-EUPOS
Sprzęt teleinformatyczny	Komputery, urządzenia sieciowe, osprzęt oraz urządzenia peryferyjne znajdujące się w centrum zarządzającym oraz na stacjach referencyjnych systemu ASG-EUPOS
Strony	Zamawiający i Wykonawca występujący łącznie
System ASG-EUPOS	Teleinformatyczny system wspomagania pomiarów satelitarnych i nawigacji
Środowisko informatyczne	Sprzęt teleinformatyczny, oprogramowanie łącza internetowe i procedury stosowane w centrum zarządzającym oraz na stacjach referencyjnych systemu ASG-EUPOS
Upoważniony pracownik	Pracownik Zamawiającego pełniący bezpośredni nadzór na funkcjonowaniem centrum zarządzającego ASG-EUPOS lub wskazany w umowie do koordynowania wsparcia informatycznego
Wsparcie informatyczne	Czynności wykonywane przez Wykonawcę na potrzeby systemu ASG-EUPOS, których przedmiot i sposób wykonania zostały opisane w SOPZ
Wykonawca	Podmiot świadczący usługi wsparcia informatycznego na rzecz Zamawiającego

Zamawiający	Główny Urząd Geodezji i Kartografii
Zgłoszenie	Wystąpienie upoważnionego pracownika lub administratora o informację, konsultację lub poradę albo zawiadomienie o wystąpieniu incydentu

2. Przedmiot zamówienia

1. Przedmiotem zamówienia jest świadczenie usługi wsparcia informatycznego w zakresie konfiguracji i konserwacji sprzętu teleinformatycznego w centrach zarządzających i na stacjach systemu ASG-EUPOS zgodnie z niniejszym opisem przedmiotu zamówienia, obejmujących w szczególności:
   1) przeprowadzenie audytu informatycznego sprzętu teleinformatycznego i oprogramowania systemu ASG-EUPOS;
   2) monitorowanie stanu sprzętu teleinformatycznego i oprogramowania w centrum zarządzającym i na stacjach referencyjnych i sporządzanie wymaganych raportów;
   3) diagnozowanie zgłaszanych incydentów, w tym określanie ich źródła, miejsca, skali i oddziaływania na funkcjonowanie systemu ASG-EUPOS;
   4) rozwiązywanie incydentów w centrum zarządzającym oraz na stacjach referencyjnych poprzez restarty lub rekonfigurację urządzeń i oprogramowania albo wymianę, w uzgodnieniu z Zamawiającym, urządzeń i oprogramowania na inne dostarczone przez Zamawiającego;
   5) instalowanie i konfigurowanie nowego sprzętu teleinformatycznego i oprogramowania oraz zmiany konfiguracji urządzeń i aktualizacja oprogramowania, w celu zapewnienia optymalnej wydajności sprzętu teleinformatycznego w centrum zarządzającym i na stacjach referencyjnych;
   6) utrzymanie techniczne strony internetowej systemu *www.asgeupos.pl;*
   7) udzielanie administratorom konsultacji w zakresie konfiguracji, optymalizacji i funkcjonowania sprzętu informatycznego i oprogramowania;
   8) udzielanie wymaganych informacji i przesyłanie miesięcznych raportów z wykonanych usług wsparcia informatycznego.
2. W ramach ogólnej odpowiedzialności Wykonawca jest zobowiązany do realizacji kompleksowych działań związanych z identyfikacją, rejestracją, kategoryzacją i priorytetyzacją incydentów, obsługą i rozwiązywaniem incydentów bądź ich delegowaniem do podmiotów trzecich, dokumentowaniem rozwiązań oraz zamykaniem wszystkich zgłoszeń.
3. Wykonawca jest zobowiązany świadczyć usługi wsparcia informatycznego:
   1) w godzinach pracy – poprzez pełnienie dyżuru bezpośrednio w centrum zarządzającym lub zdalnie oraz udzielanie konsultacji; bezpośrednio, telefoniczne lub za pomocą poczty elektronicznej, określenie centrum zarządzającego, w którym pełniony będzie dyżur leży w gestii Wykonawcy;
   2) poza godzinami pracy – poprzez działania wykonywane zdalnie oraz udzielanie konsultacji;
4. Wykonawca będzie zobowiązany do świadczenia wsparcia informatycznego w trybie 24 h/7 dni w tygodniu na warunkach określonych w kolejnych rozdziałach niniejszego dokumentu:
5. Wsparcie informatyczne będzie realizowane z wykorzystaniem istniejących procedur utrzymaniowych i eksploatacyjnych Zamawiającego za pomocą będących w posiadaniu Zamawiającego narzędzi lub procedur i narzędzi zapewnionych przez Wykonawcę, a zaakceptowanych przez Zamawiającego.
6. Rozpoczęcie usługi wsparcia informatycznego nastąpi bezpośrednio po zawarciu umowy i będzie realizowane równocześnie z prowadzeniem audytu informatycznego.

3. Warunki zamówienia

3.1. Podmioty i role

1. Główny Urząd Geodezji i Kartografii (dalej Zamawiający) jest urzędem obsługującym Głównego Geodetę Kraju, w tym prowadzącym system ASG-EUPOS oraz wykonującym czynności materialno-

techniczne służące realizacji zadań publicznych przypisanych Głównemu Geodecie Kraju, w tym mających znaczenie dla realizacji niniejszego zamówienia:

1) zapewnienie warunków do ciągłości działania sprzętu teleinformatycznego systemu ASG-EUPOS;
2) zapewnienie funkcjonowania centrum zarządzającego ASG-EUPOS;
3) obsługa zamówień na dane i usługi systemu ASG-EUPOS poprzez portal PZGiK.

3. Centrum zarządzające ASG-EUPOS jest utrzymywane przez Zamawiającego w dwóch terenowych lokalizacjach:
   1) centrum zarządzające ASG-EUPOS w Warszawie (główne), 01-102 Warszawa, ul. Olbrachta 94B (siedziba GUGiK), dalej CZWawa;
   2) centrum zarządzające ASG-EUPOS w Katowicach (zapasowe), 40-017 Katowice, ul Graniczna 29 bud. B (siedziba Bipromet S.A.), dalej CZKato;
   3) CZWawa i CZKato połączone są stałymi łączami VPN i z każdego z nich jest zapewniony pełny dostęp do środowiska informatycznego systemu ASG-EUPOS.

3.2. Teleinformatyczny system ASG-EUPOS

1. System ASG-EUPOS składa się z trzech podstawowych segmentów, którymi są: moduł stacji referencyjnych, moduł obliczeniowy oraz moduł zarządzania (centrum zarządzające). Do systemu ASG-EUPOS jest włączonych 125 stacji referencyjnych rozmieszczonych równomiernie na terenie całego kraju, w tym:
   1) 84 stacje będące własnością Zamawiającego, które są w pełni zarządzane przez administratorów ASG-EUPOS;
   2) 15 stacji należących do zewnętrznych instytucji naukowych oraz samorządowych;
   3) 26 zagranicznych stacji referencyjnych uzupełniających sieć ASG-EUPOS w strefie przygranicznej.
2. Rozmieszczenie i wyposażenie stacji referencyjnych systemu ASG-EUPOS zostało przedstawione na stronie ASG-EUPOS w zakładce: http://www.asgeupos.pl/index.php?wpg_type=syst_descr.
3. Obserwacje ze stacji referencyjnych są przesyłane do centrum zarządzającego i przetwarzane w czasie rzeczywistym celem udostępnienia użytkownikom w postaci danych korekcyjnych RTK/ DGNSS oraz zapisywane w postaci plików tekstowych RINEX na urządzeniach dyskowych w CZWawa i CZKato. Struktura systemu ASG-EUPOS pozwala na dołączanie kolejnych stacji referencyjnych oraz tworzenie nowych serwisów poprzez dodawanie jednostek sprzętu i licencji oprogramowania.

3.2.1. Moduł stacji referencyjnych

1. Głównymi elementami stacji referencyjnych są odbiorniki satelitarne wraz z antenami GNSS, które odbierają sygnały z satelitów nawigacyjnych. Na stacjach systemu ASG-EUPOS pracują odbiorniki śledzące sygnały systemów GPS, GLONASS, Galileo. Stacje referencyjne umieszczone zostały głównie w budynkach administracji publicznej, co ma zapewnić ich wieloletnią, niezakłóconą pracę. Stacje referencyjne będące własnością Zamawiającego są wyposażone w urządzenia telekomunikacyjne oraz urządzenia podtrzymujące zasilanie w przypadku awarii sieci elektrycznej, a stacje należące do sieci EPN są ponadto wyposażone w sensory meteorologiczne.
2. Dane obserwacyjne z wszystkich stacji referencyjnych wysyłane są równolegle do CZWawa i CZKato, gdzie podlegają opracowaniu. Komunikacja pomiędzy stacjami referencyjnymi należącymi do Zamawiającego a CZWawa i CZKato odbywa się poprzez sieć PESEL-NET MPLS, która zapewnia bezpieczeństwo transmisji danych oraz wymaganą przepływność i małe opóźnienia transmisji. Dane ze stacji zagranicznych oraz ze stacji stowarzyszonych są transmitowane za pomocą publicznego Internetu bez szyfrowania (i bez gwarantowanych parametrów opóźnienia i przepływności).

3.2.2. Moduł obliczeniowy

Opracowanie danych obserwacyjnych GNSS realizowane jest za pomocą oprogramowania Trimble Pivot Platform i oprogramowania APPS zainstalowanego w CZWawa i CZKato. Rozwiązanie takie zapewnia redundancję obliczeń, co umożliwia świadczenie usług w trybie 24/7/365, przy zakładanej 99,7% niezawodności i dostępności. W przypadku wystąpienia incydentu krytycznego istnieje możliwość półautomatycznego przełączenia serwisów systemu z CZWawa do CZKato i odwrotnie. W centrum

zarządzającym wszystkie urządzenia są podłączone do modułów zasilania awaryjnego w celu zminimalizowania ryzyka związanego z wystąpieniem przerw w dostawie energii elektrycznej, a w CZWawa zasilanie awaryjne dodatkowo odbywa się za pomocą generatora prądu.

3.2.3. Moduł zarządzający

Bieżącą obsługę serwisów systemu ASG-EUPOS zapewniają administratorzy, a obsługę finansowo-księgową pracownik administracyjny. Do podstawowych zadań administratorów należy bieżące monitorowanie pracy poszczególnych modułów systemu, wykonywanie niezbędnych testów infrastruktury technicznej i usług oraz prowadzenie serwisu wsparcia technicznego, celem utrzymania nieprzerwanego funkcjonowania systemu ASG-EUPOS.

3.3. Serwisy systemu ASG-EUPOS

System ASG-EUPOS świadczy usługi dla użytkowników w trybie 24/7/365, co oznacza, że urządzenia pracują nieprzerwanie w ciągu całego roku. Funkcjonalnie zostały wydzielone następujące serwisy systemu ASG-EUPOS:

1. Serwisy czasu rzeczywistego (NAWGEO, KODGIS, NAWGIS), polegające na udostępnianiu danych korekcyjnych i umożliwiające wykonywanie względnych pomiarów GNSS oraz wyznaczanie w terenie współrzędnych i wysokości punktów. Do połączenia się z tymi serwisami najczęściej wykorzystywana jest technologia transmisji danych pakietowych za pomocą sieci telefonii komórkowej GSM (GPRS/ EDGE/ UMTS/ HSDPA),
2. Serwisy postprocessingu (POZGEO POZGEO D, POZGEO DF), polegające na opracowaniu przesłanych obserwacji GNSS lub udostępnianiu obserwacji GNSS do obliczeń wykonywanych samodzielnie przez użytkowników.
3. Serwis wsparcia technicznego, polegający na udostępnianiu materiałów informacyjnych i szkoleniowych oraz udzielaniu użytkownikom systemu wszelkiego rodzaju porad technicznych. Pomoc świadczona jest drogą telefoniczną lub mailową w godzinach pracy centrum zarządzającego. W soboty w centrum zarządzającym pełniony jest dyżur administratora systemu celem monitorowania pracy modułu obliczeniowego oraz udostępniania informacji użytkownikom systemu.

3.4. Zasoby systemu ASG-EUPOS

3.4.1. Infrastruktura sprzętowa

1. W CZWawa znajduje się poniższy sprzęt informatyczny i oprogramowanie:
   1) Serwery Dell, Fujitsu i HP – łącznie 14 szt.,
   2) Firewall Fortigate – 1 szt.,
   3) Przełączniki Cisco i HP – łącznie 5szt.,
   4) Router Cisco – 1 szt.,
   5) Macierze dyskowe HP i Infotrend – łącznie 2 szt.,
   6) Urządzenia UPS Cover Partner – 2 szt.,
   7) Stacje robocze (jednostki centralne, monitory, klawiatury) – 6 szt.
   8) Komputery przenośne – 2 szt.
   9) Osprzęt i wyposażenie – drukarka sieciowa, skaner, urządzenie nagrywające, telefony, okablowanie strukturalne, listwy i zasilacze.
   10) Oprogramowanie systemowe – m.in. MS Windows Server 2003/2008/2012/2012R2/2019.
2. W CZKato znajduje się poniższy sprzęt informatyczny i oprogramowanie:
   1) Serwery Dell, Fujitsu i HP – łącznie 14szt.,
   2) Firewall Fortigate – 1 szt.,
   3) Przełączniki Cisco i HP – łącznie 5szt.,
   4) Router Cisco – 1 szt.,
   5) Macierz dyskowa HP – 1 szt.,
   6) Urządzenia UPS – 2 szt

7) Stacje robocze (jednostki centralne, monitory, klawiatury) – 8 szt
8) Komputery przenośne – 2 szt.
9) Osprzęt i wyposażenie – drukarka sieciowa, skaner, urządzenie nagrywające, telefony, urządzenia klimatyzacyjne.
10) Oprogramowanie systemowe –m.in. MS Windows Server 2003/2008/2012/2012R2/2019.

3. Na stacjach referencyjnych znajduje się poniższy sprzęt informatyczny:
   1) Firewall Juniper Netscreen 5GT
   2) UPS EATON PW 9130, 9125, 5130
   3) Konwerter TCP-IP MOXA NPort 5110
4. Rodzaj, typ, model, rok produkcji i inne szczegóły techniczne odnoszące się do poszczególnych lokalizacji lub jednostek sprzętu informatycznego i wyposażenia będą udostępnione Wykonawcy w centrum zarządzającym ASG-EUPOS.

3.4.2. Aplikacje obliczeniowe

1. Trimble Pivot Platform

Trimble Pivot Platform w wersji 4.3 jest głównym oprogramowaniem aplikacyjnym systemu ASG-EUPOS, które odpowiada za gromadzenie danych obserwacyjnych, ich przetwarzanie oraz udostępnianie w postaci danych korekcyjnych (serwisów) użytkownikom systemu. Oprogramowanie TPP pracuje w środowisku Windows i objęte jest odrębną asystą techniczną producenta oprogramowania.

2. APPS

Automatic Post Processing Software – jest to oprogramowanie aplikacyjne służące do opracowania plików GNSS użytkowników systemu ASG-EUPOS przesłanych do opracowania. APPS pracuje w środowisku Windows.

3. Microsoft SQL Server

Baza danych odpowiedzialna za prawidłowe działanie aplikacji TPP, APPS oraz internetowej strony systemu ASG-EUPOS. W CZWawa i CZKatao są osobne bazy danych, które w trakcie przełączenia usług z jednego centrum do drugiego wymagają zsynchronizowania. W trakcie trwania umowy przewidziana jest migracja bazy danych z MS SQL Server.

4. Bernese

Oprogramowanie Bernese v. 5.2 – jest to oprogramowanie aplikacyjne służące do obliczeń precyzyjnych współrzędnych stacji referencyjnych systemu ASG-EUPOS i konserwacji geodezyjnego układu odniesienia. Oprogramowanie Bernese v. 5.2 pracuje w środowisku Linux.

5. DUDE

Oprogramowanie aplikacyjne DUDE wykorzystywane jest do monitorowania urządzeń IT. Za pomocą protokołu SNMP gromadzone są informacje dotyczące stanu poszczególnych urządzeń. Oprogramowanie DUDE pracuje w środowisku Windows.

6. Portal PZGiK

Portal PZGiK służy do udostępniania usług, danych i materiałów systemu ASG-EUPOS w trybie on-line przez Internet. Portal PZGiK pracuje w środowisku Windows i powiązany jest z systemem ASG-EUPOS poprzez bazę SQL Server. Portal PZGiK objęty jest odrębną asystą techniczną.

3.5. Warstwa dostępowa

1. W środowisku informatycznym systemu ASG-EUPOS stosowane są następujące metody dostępu:
   1) dostęp do systemu przez przeglądarkę www.asgeupos.pl i http://system.asgeupos.pl;
   2) dostęp do usług czasu rzeczywistego poprzez protokół NTRIP TCP/ IP;
   3) dostęp do zbiorów danych za pomocą FTP;
   4) zdalny dostęp administracyjny poprzez tunel IPSec (VPN Point To Point).
2. W środowisku informatycznym systemu ASG-EUPOS stosowane są następujące połączenia pomiędzy komponentami systemu:

1) połączenia do stacji referencyjnych, realizowane poprzez:
   a) MPLS +VPN z gwarantowaną przepustowością i opóźnieniem – do stacji zarządzanych przez Zamawiającego,
   b) publiczny Internet (łącza dostarcza podmiot zewnętrzny) – do stacji referencyjnych zarządzanych przez podmioty zewnętrzne;
2) połączenia pomiędzy CZWawa i CZKato (łącze podstawowe i zapasowe) w technologii VPN i poprzez publiczny Internet;
3) połączenie do publicznego Internetu w celu udostępniania danych korekcyjnych poprzez GSM oraz danych obserwacyjnych za pomocą serwera FTP;
4) połączenie do sieci wewnętrznej GUGiK w celu obsługi portalu PZGiK.

3.6. Środowisko backupowe

Środowisko backupowe systemu ASG-EUPOS w CZWawa i CZKato składa się z biblioteki taśmowej Tandberg Data Storage Loader wraz z taśmami magnetycznymi oraz z serwera zarządzania backupem pracującym w środowisku Windows.

4. Zakres prac

4.1. Przeprowadzenie audytu informatycznego

4.1.1. Cel audytu

1. Celem audytu informatycznego jest inwentaryzacja sprzętu teleinformatycznego i oprogramowania, identyfikacja elementów konfiguracji i struktury środowiska informatycznego oraz zapewnienie poprawnego modelu logicznego funkcjonowania sprzętu teleinformatycznego i oprogramowania systemu ASG-EUPOS.
2. Audyt obejmie cały system ASG-EUPOS, w tym konfigurację sprzętu teleinformatycznego i jego wydajność, funkcjonalność zainstalowanego oprogramowania oraz ważność posiadanych kluczy i licencji.
3. W szczególności audyt powinien obejmować:
   1) analizę architektury sprzętu informatycznego pod kątem jego efektywności, w tym co najmniej:
      a) sprawdzenie konfiguracji poszczególnych modułów funkcjonalnych systemu,
      b) sprawdzenie zgodności stosowanego sprzętu informatycznego z jego przeznaczeniem,
      c) sprawdzenie istniejących zabezpieczeń sprzętowych i programowych,
      d) kontrolę wykorzystywania udostępnionych zasobów informatycznych przez uprawnione osoby;
   2) kontrolę zasadności dostępu do zasobów współdzielonych, w tym co najmniej:
      a) wykrycie możliwych dróg dostępu do systemu z zewnątrz,
      b) przeprowadzenie testów bezpieczeństwa informacji i prawidłowego działania backup'u,
      c) skanowanie skuteczności zapór firewall i zabezpieczeń antywirusowych,
      d) sprawdzenie bezpieczeństwa serwera www i systemu komunikacji;
   3) analizę bezpieczeństwa DNS/IPS, w tym co najmniej:
      a) sprawdzenie systemu uwierzytelniania haseł dostępowych,
      b) sprawdzenie innych, wybranych elementów systemu;
   4) przedstawienie oceny zagrożeń z opisem wykrytych problemów oraz wskazaniem działań zapobiegawczych w bliższym i dalszym horyzoncie czasowym.
4. Audyt ma odpowiedzieć na pytanie czy zasoby są wykorzystywane efektywnie i zgodnie z projektem funkcjonalnym, a dane są dostatecznie zabezpieczone przed nieautoryzowanym dostępem. Wynikiem audytu winny być zalecenia odnośnie zmian konfiguracyjnych sprzętu, zakupów sprzętu i licencji oprogramowania oraz wprowadzenia zmian lub uzupełnień do istniejących procedur i dokumentów.

5. Audyt winien być przeprowadzony w czasie 3 (trzech) miesięcy od zawarcia umowy łącznie z przekazaniem wyników audytu, w postaci raportu z audytu lub w innej uzgodnionej formie, Zamawiającemu.
6. Zamawiający, w miarę swoich możliwości, uwzględni zalecenia Wykonawcy dotyczące konfiguracji, rozbudowy i eksploatacji sprzętu teleinformatycznego.

4.1.2. Audyt sprzętu

1. Audyt powinien objąć sprawdzenie parametrów technicznych jednostek sprzętowych istotnych dla funkcjonowania systemu ASG-EUPOS, ich zadań i konfiguracji technicznej oraz współdziałania z innymi elementami środowiska informatycznego systemu.
2. Audyt ma dać informację czy konfiguracja urządzeń jest zgodna z dokumentacją powykonawczą (z późniejszymi modyfikacjami), a także, czy urządzenia mają wymagane podzespoły.
3. Wynik audytu powinien umożliwić zaplanowanie zmian w konfiguracji sprzętu informatycznego oraz wskazać listę niezbędnych zakupów sprzętu teleinformatycznego.

4.1.3. Audyt oprogramowania

1. Audyt powinien objąć systemy operacyjne oraz oprogramowanie używane na serwerach i stacjach roboczych oraz wykorzystanie procesorów, pamięci RAM i przestrzeni dyskowej urządzeń. Niezbędne będzie wyszukanie i wskazanie programów i aplikacji nie mających związku z wykonywanymi zadaniami.
2. Wynik audytu powinien wskazać oprogramowanie niepożądane lub nadmiernie obciążające procesory oraz umożliwić dokonanie zmian w konfiguracji uniemożliwiających instalację takiego oprogramowania.

4.1.4. Audyt bezpieczeństwa

1. Audyt ma ustalić podatność środowiska informatycznego na zagrożenia, a także czy wykorzystywane zabezpieczenia sprzętowe i programowe oraz procedury są bezpieczne, oprogramowanie jest aktualne i ma ważne licencje, a także czy administratorzy mają odpowiednie prawa dostępu.
2. Należy sprawdzić czy nie występują luki w zabezpieczeniach oraz nieuprawnione połączenia z systemem lub próby takich połączeń.
3. Wynik audytu powinien wskazać na zagrożenia bezpieczeństwa, zawierać proponowane zmiany w procedurach bezpieczeństwa oraz zalecenia dotyczące wdrożenia narzędzi i procesów poprawiających bezpieczeństwo.

4.2. Obsługa zgłoszeń

1. Wykonawca zapewni uruchomienie systemu przyjmowania zgłoszeń lub service-desku (dalej system zgłoszeń) czynnego 7 dni w tygodniu, 24 godziny na dobę.
2. System zgłoszeń stanowi punkt kontaktu upoważnionych pracowników Zamawiającego lub administratorów z Wykonawcą we wszystkich sprawach związanych ze wsparciem informatycznym.
3. System zgłoszeń winien zapewnić:
   1) przyjmowanie, rejestrowanie i ewidencja zgłoszeń z wykorzystaniem wszystkich dostępnych kanałów komunikacji;
   2) udzielanie informacji lub konsultacji w zakresie sprzętu teleinformatycznego i oprogramowania;
   3) kierowanie zgłoszeń do zespołów lub pracowników Wykonawcy lub podmiotów trzecich;
   4) raportowanie obsługi zgłoszeń i incydentów
4. Zgłoszenia będą przekazywane:
   1) telefonicznie;
   2) za pomocą poczty elektronicznej.
5. Dopuszcza się składanie zgłoszeń za pomocą strony internetowej lub formularza zgłoszeniowego, jeżeli Wykonawca dysponuje internetowym systemem zarządzania incydentami.
6. Zgłoszenie będzie zawierać w szczególności opis incydentu (zdarzenia) oraz w miarę możliwości opis okoliczności jego wystąpienia.

4.3. Diagnozowanie incydentów

1. Celem procesu jest zminimalizowanie negatywnego wpływu incydentów na działania klientów korzystających z usług systemu ASG-EUPOS oraz jak najszybsze przywracanie funkcjonowania usług zachwianych przez incydenty.
2. W ramach procesu, Wykonawca będzie odpowiedzialny za realizację następujących aktywności:
   1) identyfikowanie i rejestrowanie incydentów;
   2) badanie i diagnozowanie incydentów;
   3) priorytetyzację incydentów krytycznych;
   4) przygotowanie wniosków o podjęcie działań dla przygotowanych rozwiązań jeśli wymagają one formalnego uruchomienia procesu zarządzania zmianą;
   5) delegowanie incydentów do pracowników Wykonawcy lub podmiotów trzecich;
   6) sprawdzenie funkcjonalności modułów środowiska informatycznego zachwianej przez incydenty;
   7) opracowywania modeli (procedur) rozwiązywania incydentów dla najczęstszych typów incydentów;
   8) bieżące informowanie Zamawiającego o postępie w obsłudze incydentów, raportowanie obsługi incydentów.

4.4. Rozwiązywanie incydentów

1. Celem procesu jest opracowanie rozwiązań tymczasowych i docelowych zmierzających do jak najszybszego usunięcia przyczyn incydentów oraz zarządzanie działaniami zmierzającymi do redukcji liczby incydentów w przyszłości.
2. Wykonawca w pierwszej kolejności będzie realizował czynności zmierzające do usunięcia incydentów krytycznych.
3. W ramach procesu Wykonawca będzie odpowiedzialny za realizację następujących aktywności:
   1) inicjowanie wprowadzania opracowanych rozwiązań i usuwanie wpływu incydentów na funkcjonowanie środowiska informatycznego;
   2) prowadzenie działań mających na celu zapobieganie występowania incydentów zgodnie z ustalonymi modelami lub pojedynczych incydentów o dużym wpływie na środowisko informatyczne;
   3) dokumentowanie rozwiązań dla incydentów i rejestrowanie potencjalnych usprawnień zmierzających do zmniejszenia liczby incydentów w przyszłości;
   4) utrzymywanie dziennika zdarzeń oraz udostępnianie i przyjmowanie informacji od podmiotów trzecich uczestniczących w rozwiązywaniu incydentów;
   5) eskalowanie badania, diagnozy i rozwiązywania incydentów, które dotyczą elementów środowiska informatycznego pozostających poza odpowiedzialnością Wykonawcy (np. błędy w oprogramowaniu, procedurach, itd.);
   6) wypełnienie protokołu uszkodzeń sprzętu teleinformatycznego z opisem uszkodzeń i zaleceniami dotyczącymi dalszy działań.
4. Wszelkie próby rozwiązania incydentów na stacjach referencyjnych Wykonawca będzie prowadził zdalnie (Wykonawca nie będzie zobowiązany do wyjazdów na stacje referencyjne).
5. Zamknięcie incydentu następuje po potwierdzeniu przez Zamawiającego usunięcia problemów w funkcjonowaniu środowiska informatycznego.
6. W ramach procesu diagnozowania i rozwiązywania incydentów Wykonawca jest zobowiązany do bieżącego utrzymania dokumentów wymienionych w tabeli 2.

Tabela 2. Dokumentacja zarządzania incydentami

Lp.	Nazwa	Opis / ramowy zakres	Termin przekazania
1.	Definicja procesu	Dokumentacja powykonawcza, opis procesu obejmujący co najmniej jego cel, politykę, wyzwalacze, diagram z przebiegiem, opis kroków, opis ról i odpowiedzialności produkty, kluczowe procedury i instrukcje	W terminie 14 dni od modyfikacji
2.	Informacja z diagnozowania	Dziennik zdarzeń, opis incydentu obejmujący przyczynę i oddziaływanie oraz priorytet	Niezwłocznie po rozwiązaniu incydentu
3.	Informacja z rozwiązania	Dziennik zdarzeń, opis działań, uczestnicy, uzyskane efekty, zalecenia	
4.	Model incydentów	Dokumentacja powykonawcza, opis procedur obejmujący co najmniej symptomy (wyzwalacze), opis przebiegu (czynności), opis odpowiedzialności, oczekiwany efekt.	W terminie 14 dni od przetestowania

4.5. Zarządzanie zasobami ASG-EUPOS

4.5.1. Monitorowanie środowiska informatycznego

1. Monitorowanie środowiska informatycznego i analiza danych monitorowania ma umożliwić wykrywanie potencjalnych zagrożeń i stanowi podstawę do podejmowania działań związanych z bieżącym utrzymaniem i eksploatacją sprzętu teleinformatycznego i oprogramowania oraz wprowadzaniem zmian.
2. Monitorowanie będzie realizowane za pomocą narzędzi udostępnione przez Zamawiającego i narzędzi Wykonawcy, z zachowaniem bezpieczeństwa systemu ASG-EUPOS.
3. W ramach procesu Wykonawca będzie odpowiedzialny za realizację następujących aktywności:
   1) projektowanie i utrzymanie procesów monitorowania, w tym opracowanie propozycji nowych mierników, strojenie, dostosowanie i konfigurację narzędzi monitorowania oraz wprowadzanie zaakceptowanych przez Zamawiającego zmian;
   2) bieżące monitorowanie środowiska informatycznego (w tym dokonywanie przeglądów logów systemowych i dokonywanie optymalizacji działania);
   3) projektowanie i aktualizowanie procedur wykrywania i rejestracji zagrożeń wynikających ze zmian statusów elementów konfiguracji środowiska informatycznego;
   4) projektowanie i aktualizowanie reguł generowania powiadomień dla zagrożeń (ang. *warning*);
   5) filtrowanie i kategoryzacja zagrożeń oraz prowadzenie oceny ryzyka;
   6) zarządzanie wykonywaniem działań zatwierdzonych do realizacji w wyniku pojawiania się określonych zagrożeń (np. opracowanie skryptów do automatycznej reakcji na zdarzenia, itd.);
   7) sporządzanie okresowych raportów i aktualizacja dokumentacji powykonawczej systemu ASG-EUPOS.
7. Minimalne zobowiązania Wykonawcy w obszarze monitorowania i zarządzania incydentami zawiera tabela 3.

Tabela 3. Parametry SLA dla obszaru monitorowania i zarządzania incydentami

Lp.	Parametr	Rodzaj incydentu/ oczekiwana wartość		
		krytyczny	**pilny**	**standardowy**
1.	Czas reakcji na incydent	15 min.	30 min	1h
2.	Czas rozwiązania incydentu	4h	8h	24h
3.	Czas udokumentowania rozwiązania incydentu	2 dni robocze		
4.	Czas opracowania modelu postępowania dla incydentu	7 dni roboczych		

5.	Częstotliwość przeglądu i analizy incydentów	co najmniej 1 raz w tygodniu
6.	Czas zarejestrowania incydentu w dzienniku zdarzeń	niezwłocznie po rozwiązaniu incydentu
7.	Czas wdrożenia modelu postępowania dla incydentu	uzgodniony z Zamawiającym

8. Wykonawca będzie uwzględniał spełnienie wymagań podanych w tabeli 3 w sporządzanych przez siebie raportach i zgodnie z nimi będzie rozliczany.

4.5.2. Zarządzanie zasobami

1. Celem procesu jest zapewnienie ciągłości działania systemu ASG-EUPOS poprzez podejmowanie czynności technicznych a w uzgodnieniu z Zamawiającym także czynności administracyjnych niezbędnych do utrzymania dostępności i wydajności środowiska informatycznego.
2. Wykonawca będzie wspierał Zamawiającego w zarządzaniu dostępnością i pojemnością środowiska informatycznego poprzez monitorowanie, zapewnienie dostępności sprzętu teleinformatycznego oraz przygotowywanie analiz i prognoz co do wykorzystania i ewentualnej rozbudowy sprzętu teleinformatycznego i oprogramowania.
3. W ramach procesu Wykonawca będzie odpowiedzialny za realizację następujących aktywności:
   1) utrzymywanie uzgodnionego z Zamawiającym poziomu dostępności i wydajności sprzętu teleinformatycznego poprzez:
      a) administrowanie, konfigurację, strojenie i utrzymanie sprzętu teleinformatycznego,
      b) monitorowanie ryzyk zachwiania ustalonego poziomu dostępności i wydajności sprzętu teleinformatycznego,
      c) prognozowanie i informowanie z wyprzedzeniem Zamawiającego o potencjalnych zagrożeniach z dostępnością i wydajnością,
      d) wykonywanie konserwacji i napraw sprzętu teleinformatycznego we własnym zakresie lub po uzgodnieniu z Zamawiającym - przekazywaniu do serwisu z opisem uszkodzenia, jeśli sprzęt (osprzęt) jest na gwarancji lub naprawa we własnym zakresie jest niemożliwa, oraz jego rekonfigurowaniu po naprawie,
      e) instalowanie nowo zakupionego sprzętu teleinformatycznego i oprogramowania oraz przenoszenie sprzętu i oprogramowania,
      f) wykonywanie archiwizacji danych oraz tworzenie kopii bezpieczeństwa;
      g) przygotowanie opisu zmian i propozycji rozwiązań, w tym projektów rozbudowy środowiska informatycznego;
   2) bieżące monitorowanie środowiska informatycznego oraz raportowanie o dostępności usług, wydajności procesów oraz obciążeniu elementów sprzętu teleinformatycznego;
   3) utrzymywanie aktualnej informacji o licencjach i gwarancjach dotyczących sprzętu teleinformatycznego i oprogramowania;
   4) podejmowanie działań mających na celu zapobieganie przeciążeniu elementów sprzętu teleinformatycznego
   5) zgłaszanie z wyprzedzeniem zapotrzebowania na zakup sprzętu, licencji lub aktualizacji niezbędnych elementów środowiska informatycznego, opracowanie opisów oraz określanie parametrów technicznych i eksploatacyjnych potrzebnego sprzętu teleinformatycznego, oprogramowania i materiałów na potrzeby zamówień publicznych;
   6) wykonywaniu innych działań zapewniających sprawność sprzętu teleinformatycznego i oprogramowania, w tym:
      a) dokonywanie doraźnych zakupów akcesoriów i materiałów eksploatacyjnych do sprzętu teleinformatycznego na koszt Zamawiającego i zgodnie z jego wytycznymi,
      b) przygotowywanie sprzętu teleinformatycznego do pracy (konfiguracja, uzupełnianie materiałów eksploatacyjnych).
4. Wykonawca będzie zobowiązany do współdziałania z podmiotami trzecimi odpowiedzialnymi za opiekę gwarancyjną lub asystę pogwarancyjną elementów środowiska informatycznego. Współdziałanie będzie obejmowało w szczególności uczestnictwo w spotkaniach, weryfikację produktów, opracowanie opinii i rekomendacji oraz uczestnictwo w pracach związanych z wdrażaniem rozwiązań, sprzętu i oprogramowania.

5. Szczegółowe zestawienie odpowiedzialności Wykonawcy w ramach zarządzania zasobami oraz utrzymania i eksploatacji sprzętu teleinformatycznego i oprogramowania zawiera tabela 4.

Tabela 4. Zestawienie odpowiedzialności Wykonawcy w ramach utrzymania i eksploatacji sprzętu informatycznego i oprogramowania

Obszary kompetencyjne	Nazwa czynności
Obszar aplikacyjny (oprogramowanie standardowe i dedykowane)	Instalowanie oprogramowania, w szczególności wgrywanie aktualizacji oprogramowania systemowego i użytkowego
	Monitorowanie w zakresie incydentów bezpieczeństwa, w szczególności przegląd alarmów bezpieczeństwa i logów systemowych
	Diagnozowanie problemów w działaniu aplikacji obliczeniowych
	Przygotowanie i testowanie nowych środowisk aplikacyjnych
	Rekonfigurowanie istniejących środowisk aplikacyjnych
Obszar wirtualizacji	Konfigurowanie środowiska wirtualizacyjnego, w szczególności zmiana parametrów ustawień, konfiguracja switch'y wirtualnych, tworzenie nowych maszyn wirtualnych, konfiguracja przydziału pamięci i mocy obliczeniowej
	Monitorowanie i optymalizowanie działania środowiska wirtualizacyjnego
Obszar systemów operacyjnych	Instalowanie oprogramowania systemowego, w szczególności wgrywanie aktualizacji oprogramowania systemowego, monitorowanie ważności licencji
	Monitorowanie w zakresie incydentów bezpieczeństwa, w szczególności przegląd alarmów bezpieczeństwa i logów systemowych
	Monitorowanie i optymalizowanie procesów obliczeniowych (parametryzacja, przegląd kolejek itp.)
Obszar infrastruktury serwerowej	Konfigurowanie urządzeń (wprowadzanie parametrów pracy do urządzeń)
	Monitorowanie parametrów działania urządzeń, w szczególności monitorowanie wydajności, temperatury, stanu sprzętu, pojemności
	Monitorowanie w zakresie incydentów bezpieczeństwa, w szczególności przegląd alarmów bezpieczeństwa i logów systemowych
	Aktualizowanie oprogramowania typu firmware, w szczególności wgrywanie aktualizacji oprogramowana do urządzeń, testowanie działania urządzeń
	Instalowanie urządzeń (urządzenia nowe i urządzenia po wymianie, wymiana wadliwego sprzętu, zabezpieczenie wadliwego sprzętu wg polityki bezpieczeństwa informacji)
	Raportowanie incydentów związanych z naruszeniem bezpieczeństwa
Obszar bazy danych	Monitorowanie i optymalizowanie baz danych, w tym wykrywanie „wąskich gardeł", przydział pamięci operacyjnej i masowej, monitoring pojemności, strojenie, monitorowanie kompletności danych
	Monitorowanie parametrów działania urządzeń, w szczególności monitorowanie wydajności, temperatury, stanu sprzętu, pojemności
	Monitorowanie serwerów baz danych (ocena wydajności i pojemności instancji baz danych)
	Monitorowanie w zakresie incydentów bezpieczeństwa, w szczególności przegląd alarmów bezpieczeństwa i logów systemowych
	Zarządzanie bazami danych, w szczególności rekonfiguracja parametrów, partycjonowanie baz danych, przydzielanie zasobów
	Zarządzania instancjami bazy danych (rekonfigurowanie parametrów instancji bazy danych)
	Aktualizowanie oprogramowania typu firmware i oprogramowania aplikacyjnego, w szczególności wgrywanie aktualizacji oprogramowania do urządzeń, testowanie działania urządzeń po aktualizacji
	Instalowanie urządzeń (urządzenia nowe i urządzenia po wymianie, wymiana wadliwego sprzętu, zabezpieczenie wadliwego sprzętu wg polityki bezpieczeństwa informacji)

Obszar storage (macierze)	Konfigurowanie urządzeń w ramach warstwy (wprowadzenie parametrów pracy do urządzeń)
	Monitorowanie parametrów działania urządzeń, w szczególności monitorowanie wydajności, temperatury, stanu sprzętu, pojemności
	Monitorowanie wydajności urządzeń warstwy storage (identyfikacja „wąskich gardeł", strojenie)
	Zarządzanie zasobami storage (tworzenie nowych zasobów, rekonfiguracja)
	Optymalizowanie sieci SAN, w szczególności rekonfigurowanie parametrów urządzeń sieciowych
	Monitorowanie w zakresie incydentów bezpieczeństwa, w szczególności przegląd alarmów bezpieczeństwa i logów systemowych, weryfikacja kompletności danych
	Aktualizowanie oprogramowania typu firmware, w szczególności wgrywanie aktualizacji oprogramowana do urządzeń, testowanie działania urządzeń po aktualizacji
Obszar sieci	Instalowanie urządzeń (urządzenia nowe i urządzenia po wymianie, wymiana wadliwego sprzętu, zabezpieczenie wadliwego sprzętu wg polityki bezpieczeństwa)
	Konfigurowanie urządzeń (wprowadzanie parametrów pracy do urządzeń)
	Konfigurowanie urządzeń HSM, w szczególności generowanie kluczy i wgrywanie certyfikatów
	Implementowanie zasad polityki bezpieczeństwa urządzeń sieciowych, konfigurowanie urządzeń sieciowych (firewall, switch, VPN)
	Monitorowanie parametrów działania urządzeń, w szczególności monitorowanie wydajności, temperatury, stanu sprzętu, pojemności
	Monitorowanie w zakresie incydentów bezpieczeństwa (przegląd alarmów bezpieczeństwa i logów systemowych)
	Monitorowanie wydajności sieci i dostępu do Internetu (monitorowanie NLB, obciążenia routerów i switch'y, styku ISP)
	Optymalizowanie sieci LAN, w szczególności przydzielanie adresów, partycjonowanie sieci, rekonfiguracja urządzeń
	Zarządzanie bazą użytkowników VPN, w szczególności tworzenie, modyfikowanie, usuwanie użytkowników, nadawanie i odbieranie praw dostępu do VPN, implementowanie wymagań polityki bezpieczeństwa informacji
	Monitorowanie i optymalizowanie rozwiązania równoważenia obciążenia sieciowego – NLB, w tym parametryzowanie rozwiązania
	Aktualizowanie oprogramowania typu firmware, w szczególności wgrywanie aktualizacji oprogramowana do urządzeń, testowanie działania urządzeń po aktualizacji
Obszar środowiska backupowego	Konfigurowanie i utrzymanie systemu backupu, w szczególności wgrywanie licencji, konfigurowanie scenariuszy archiwizowania danych, przyrostu danych.
	Rozszerzanie środowiska o nowe zasoby (urządzenia, taśmy, dyski).
	Konfigurowanie urządzeń (wprowadzenie parametrów pracy do urządzeń)
	Monitorowanie parametrów działania urządzeń, w szczególności monitorowanie wydajności, temperatury, stanu sprzętu, pojemności
	Aktualizowanie oprogramowania typu firmware, w szczególności wgrywanie aktualizacji oprogramowana do urządzeń, testowanie działania urządzeń po aktualizacji
	Instalowanie i utrzymanie urządzeń (urządzenia nowe i urządzenia po wymianie, wymiana wadliwego sprzętu, zabezpieczenie wadliwego sprzętu wg polityki bezpieczeństwa)
	Monitorowanie parametrów działania urządzeń, w szczególności monitorowanie wydajności, temperatury, stanu sprzętu, pojemności
	Monitorowanie w zakresie incydentów bezpieczeństwa, w szczególności przegląd alarmów bezpieczeństwa i logów systemowych

6. W przypadkach, gdy Zamawiający ma zawartą umowę z podmiotem trzecim obejmującą gwarancje na dostarczane elementy środowiska informatycznego, odpowiedzialność za realizację całości lub

części czynności wymienionych w tabeli 4 (instalacja aktualizacji, testowanie, konfiguracja) będzie ponosił właściwy podmiot trzeci. W przypadku podjęcia działań przez podmiot trzeci Wykonawca jest odpowiedzialny za określenie ram dla działań podmiotu realizującego działania, koordynację jego działań oraz wsparcie Zamawiającego w czynnościach odbioru wyników tych działań.

7. Zobowiązania Wykonawcy w ramach zarządzania zasobami oraz utrzymania środowiska informatycznego określa tabela 5. W przypadku fizycznych awarii sprzętu nie wynikających z działań Wykonawcy, jest on zwolniony od dotrzymania poniższych parametrów, do czasu naprawy/wymiany uszkodzonego sprzętu.

Tabela 5. Parametry SLA dla obszaru zarządzania zasobami i utrzymania środowiska informatycznego

Lp.	Parametr	Wymagalność/ Oczekiwana wartość		
		dzienna	**miesięczna**	**roczna**
1.	Dostępność serwerów fizycznych	97%	99%	99,7%
2.	Dostępność przestrzeni dyskowych	97%	99%	99,7%
3.	Dostępność baz danych	97%	99%	99,7%
4.	Dostępność urządzeń sieciowych	97%	99%	99,7%
5.	Dostępność systemów backupowych	97%	99%	99,7%
6.	Dostępność serwerów wirtualnych	97%	99%	99,7%
7.	Dostępność narzędzi Service Desk i monitoringu	97%	99%	99,7%
8.	Dostępność aplikacji i narzędzi standardowych	97%	99%	99,7%
9.	Dostępność usług zewnętrznych systemu	97%	99%	99,7%

4.5.3. Zarządzanie zmianami

1. Wykonawca będzie zarządzał wprowadzaniem zmian w środowisku informatycznym, obejmujących:
   1) zmiany eksploatacyjne i utrzymaniowe związane usuwaniem bieżących awarii oraz instalacją; konfiguracją i uruchamianiem sprzętu teleinformatycznego i oprogramowania;
   2) zmiany rozwojowe wynikające z planów wprowadzania w środowisku informatycznym sprzętu oprogramowania i wyposażenia;
2. Wprowadzenie zmian będzie się odbywało zgodnie z przygotowanymi przez Wykonawcę i zatwierdzonymi przez Zamawiającego procedurami.
3. Zamawiający planuje w okresie realizacji zamówienia wprowadzenie następujących zmian w systemie ASG-EUPOS:
   1) wirtualizację środowiska w centach zarządzających;
   2) wdrożenie nowych serwerów domeny oraz bazy danych MSSQL;
   3) optymalizacja środowiska w związku z wdrożeniem nowych serwerów (po dwa serwery na CZ) i zwolnieniem zasobów obecnie wykorzystywanych na ten cel maszyn;
   4) integrację sieci biurowej systemu ASG-EUPOS z siecią GUGiK.
4. Zobowiązania Wykonawcy w obszarze zarządzania zasobami i zmianami zawiera tabela 6.

Tabela 6. Parametry SLA dla obszaru zarządzania zasobami i zmianami

Lp.	Parametr	Rodzaj parametru/ Oczekiwana wartość	
1.	Monitorowanie środowiska informatycznego	co najmniej 1 raz dziennie[1)]	
2.	Monitorowanie bazy licencji i gwarancji	co najmniej 1 raz w miesiącu	
3.	Zarządzanie zmianami	**pilne**	**standardowe**
4.	Czas oceny zmiany	1 godz.	do 1 dnia roboczego

5.	Czas obsługi zmiany	3 godz.	uzgodniony z Zamawiającym
6.	Aktualizacja dokumentacji po wprowadzeniu zmiany	7 dni roboczych	
7.	Testowanie planów awaryjnych i procedur	co najmniej 1 raz na miesiąc	
8.	Przeglądów planów awaryjnych i procedur (zapewnienie ciągłości)	co najmniej 1 raz na kwartał	

[1)] dodatkowo po każdorazowym rozwiązaniu zgłoszonego incydentu

4.6. Utrzymanie spójności środowiska informatycznego

1. Celem procesu jest zapewnienie spójności środowiska informatycznego i zapewnienie kompatybilności poszczególnych elementów oraz zachowanie poprawnej konfiguracji sprzętu teleinformatycznego.
2. W ramach procesu Wykonawca będzie realizował następujące aktywności:
   1) przygotowanie i opracowanie zmian w środowisku informatycznym w zakresie odpowiedzialności Wykonawcy;
   2) opiniowanie propozycji zmian do środowisko informatycznego pod kątem ich wpływu na funkcjonalność systemu ASG-EUPOS;
   3) weryfikacja kompletności proponowanych rozwiązań pod względem możliwości ich wdrożenia i utrzymania;
   4) przygotowanie środowiska testowego i produkcyjnego dla wdrażanych zmian;
   5) wdrożenie zmian w środowisku produkcyjnym lub wsparcie eksperckie w procesie odbioru zmian wdrażanych przez podmioty trzecie, w tym;
      a) dostosowanie i konfigurowanie sprzętu teleinformatycznego,
      b) instalowanie i konfigurowanie oprogramowania,
      c) aktualizowanie konfiguracji sprzętu teleinformatycznego i oprogramowania,
      d) udostępnienie administratorom niezbędnej dla ich działania informacji;
   6) Utrzymanie i aktualizowanie dokumentacji systemu ASG-EUPOS z zastosowaniem notacji, formatów i narzędzi wykorzystywanych w ramach całej dokumentacji.

4.7. Udzielanie konsultacji

1. Konsultacje będą polegały na udzielaniu administratorom i upoważnionym pracownikom informacji i porad, bezpośrednio lub za pomocą telefonu, lub poczty elektronicznej, w zakresie konfiguracji, optymalizacji i funkcjonowania sprzętu teleinformatycznego i oprogramowania.
2. Wykonawca zobowiązany jest zapewnić udzielanie konsultacji:
   1) w dni robocze – niezwłocznie, nie później jednak niż w ciągu 1 godz. od zgłoszenia;
   2) w dni wolne od pracy i święta – w ciągu 8 godz. od zgłoszenia, nie później jednak niż o godz. 8.00 najbliższego dnia roboczego.
3. Zgłaszanie potrzeby konsultacji będzie się odbywało w sposób określony dla zgłaszania incydentów.
4. Zamawiający zastrzega sobie prawo udziału pracowników Zamawiającego w pracach związanych w wykonywaniem przedmiotu zamówienia.

4.8. Raportowanie

1. Wykonawca w ramach realizacji zamówienia jest zobowiązany do składania okresowych raportów z działań podejmowanych w ramach wsparcia informatycznego w zakresie:
   1) monitorowania środowiska informatycznego;
   2) utrzymania środowiska informatycznego;
   3) rozwiązywania incydentów;
   4) bezpieczeństwa informacji;

5) innych obszarów uznanych przez Strony za istotne dla realizacji zamówienia.

2. W przypadku potrzeby zmian zasad współpracy w toku realizacji zamówienia stosowany będzie analogiczny tryb i terminy jak dla modyfikacji obowiązujących już dokumentów.

5. Bezpieczeństwo informacji

1. Wykonawca będzie uczestniczył w zarządzaniu bezpieczeństwem informacji zgodnie ze standardami bezpieczeństwa teleinformatycznego oraz procedurami bezpieczeństwa informacji, współpracując z osobami odpowiedzialnymi za obszar bezpieczeństwa informacji Zamawiającego.
2. W ramach procesu Wykonawca będzie odpowiedzialny za realizację następujących aktywności:
   1) wykonywanie analizy i oceny ryzyka, w tym:
      a) identyfikowanie zagrożeń i podatności środowiska informatycznego na zagrożenia,
      b) oceny ryzyk związanych ze zidentyfikowanymi zagrożeniami oraz sposób postępowania z ryzykiem szczątkowym;
   2) monitorowanie poziomu bezpieczeństwa systemów m.in. poprzez:
      a) weryfikację integralności i dostępności danych i informacji gromadzonych w środowisku informatycznym,
      b) rozwiązywanie incydentów bezpieczeństwa,
      c) weryfikację podmiotów trzecich poprzez kontrolę uprawnień oraz kontrolę dostarczanego sprzętu teleinformatycznego i oprogramowania,
      d) sprawdzanie sprzętu informatycznego i oprogramowania pod względem realizowanych procesów,
      e) informowanie Zamawiającego o potrzebie zapewnienia obsługi gwarancyjnej i pogwarancyjnej sprzętu informatycznego i oprogramowania;
   3) prowadzenie okresowych testów penetracyjnych, pozwalających wykryć i załatać luki w systemie zabezpieczeń;
   4) utrzymywanie w aktualności dokumentacji bezpieczeństwa informacji, w tym polityki bezpieczeństwa i procedur bezpieczeństwa w zakresie utrzymywanych elementów środowiska informatycznego.
3. Operacyjne zarządzanie uprawnieniami dostępu do środowiska informatycznego pozostaje w odpowiedzialności Zamawiającego

6. Zobowiązania Stron

6.1. Dodatkowe zobowiązania Zamawiającego

1. Zamawiający zapewni Wykonawcy w zakresie niezbędnym do świadczenia usług wsparcia informatycznego i zgodnie z wewnętrznymi regulacjami Zamawiającego w zakresie bezpieczeństwa:
   1) dostęp bezpośredni do obiektów, sprzętu teleinformatycznego, oprogramowania oraz dokumentacji powykonawczej systemu ASG-EUPOS;
   2) stanowisko pracy osobie pełniącej dyżur z dostępem do środowiska informatycznego systemu ASG-EUPOS oraz do Internetu;
   3) dostęp zdalny do środowiska informatycznego z zachowaniem obowiązujących procedur.
2. Zamawiający będzie udzielał Wykonawcy na bieżąco wyjaśnień oraz przekazywał informacje w zakresie niezbędnym do świadczenia usług wsparcia informatycznego.
3. Zamawiający w okresie trwania wsparcia informatycznego będzie informował Wykonawcę z niezbędnym wyprzedzeniem o zamiarze podłączenia dodatkowego sprzętu teleinformatycznego, instalacji dodatkowego oprogramowania lub wprowadzenia istotnych zmian do środowiska informatycznego.

6.2. Dodatkowe zobowiązania Wykonawcy

1. Wszelkie działania Wykonawcy w ramach realizacji przedmiotu zamówienia będą oparte o uznane standardy i metodyki wykorzystywane w obszarze wsparcia informatycznego. Wykonawca będzie realizował zamówienie z najwyższą starannością, efektywnością oraz zgodnie z najlepszą praktyką i wiedzą zawodową.
2. Wykonawca zobowiązany będzie dokonać z Zamawiającym, z niezbędnym wyprzedzeniem, wszelkich koniecznych ustaleń mogących wpływać na realizację zamówienia.
3. Wykonawca zobowiązany będzie stosować się do wytycznych bezpieczeństwa systemów IT oraz do procedur bezpieczeństwa informacji stosowanych przez Zamawiającego; wytyczne i procedury zostaną przekazane po podpisaniu umowy.
4. Wykonawca zobowiązany będzie do utrzymania w aktualności dokumentów udostępnionych przez Zamawiającego jak i wytworzonych przez Wykonawcę w ramach realizacji zamówienia.
5. Wykonawca będzie udzielał Zamawiającemu okresowo lub na wniosek Zamawiającego informacji na temat stanu realizacji zamówienia zgodnie z obowiązującą Strony procedurą.
6. Wykonawca zobowiązany będzie do zapewnienia we własnym zakresie dodatkowych narzędzi do monitorowania środowiska informatycznego, innych niż będące w posiadaniu Zamawiającego, w przypadkach, gdy uzna je za niezbędne do realizacji zamówienia. Wykonawca przed zastosowaniem własnych narzędzi zobowiązany będzie do uzyskania akceptacji Zamawiającego.

7. Postanowienia końcowe

1. Wszelkie dane i informacje wytwarzane przez Wykonawcę w ramach realizacji zamówienia są własnością Zamawiającego (dotyczy to w szczególności danych i informacji gromadzonych w procesie monitorowania).
2. Wykonawca zachowa w tajemnicy wszelkie dane autoryzacyjne (identyfikatory, logi systemowe i hasła) służące do dostępu do środowiska informatycznego, a także dane i raporty oraz dane o użytkownikach i administratorach systemu ASG-EUPOS oraz zastosuje wszelkie dostępne środki, aby zapobiec ich nieuprawnionemu ujawnieniu lub wykorzystaniu.
3. Wykonawca jest zobowiązany do zrealizowania zamówienia zgodnie z ogólnopolskim standardem dotyczącym zarządzania bezpieczeństwem informacji oraz prowadzić działania związane z realizacją zamówienia zgodnie z dobrymi praktykami ITIL w wersji 3.0, normą ISO 20000 lub innym dokumentem równoważnym.
4. Dokumentacja techniczna powinna być przekazana w formie elektronicznej, wszystkie dokumenty źródłowe, które zostały wykonane w wersji analogowej, powinny być przetworzone do formy elektronicznej przy jednoczesnym zachowaniu i przekazaniu oryginałów.
5. Raport z audytu informatycznego i analizę wyników przeprowadzonych testów (pomiarów), niezależnie od postaci elektronicznej, należy przedstawić w 2 egzemplarzach w formie drukowanej.