Szczegółowy Opis Przedmiotu Zamówienia

Dostawa, utrzymanie oraz zapewnienie ciągłości działania infrastruktury w ramach projektów CAPAP, ZSIN – Faza II, K-GESUT

Spis treści

Spis tabel

Spis rysunków

1 Wstęp

Niniejszy dokument opisuje przedmiot zamówienia dostarczanego przez Wykonawcę realizowanego w ramach postępowania „*Dostawa, utrzymanie oraz zapewnienie ciągłości działania infrastruktury w ramach projektów CAPAP, ZSIN – Faza II, K-GESUT*”.

1.1 Struktura dokumentu

Poniżej przedstawiona jest struktura dokumentu wraz z krótkim opisem charakteryzującym każdy z rozdziałów:

Rozdział 1 – jest wprowadzeniem do dokumentu i opisuje niniejszą strukturę dokumentu.

Rozdział 2 - opisuje najważniejsze pojęcia stosowane w niniejszym dokumencie.

Rozdział 3 - opisuje ramy formalno-prawne (w tym kontekst projektów) w jakim realizowane jest działanie „*Dostawa, utrzymanie oraz zapewnienie ciągłości działania infrastruktury w ramach projektów CAPAP, ZSIN – Faza II, K-GESUT*”.

Rozdział 4 - opisuje sposób organizacji zamówienia. W tym strukturę organizacyjną projektów.

Rozdział 5 - definiuje przedmiot zamówienia oraz wskazuje kluczowe terminy realizacji.

Rozdział 6 - opisuje systemy informatyczne SIG

Rozdział 7 - opisuje posiadaną przez Zamawiającego infrastrukturę sprzętowo-programową oraz ośrodki przetwarzania danych

Rozdział 8 - przedstawia wizję docelową rozwiązania

Rozdział 9 - opisuje wymagania na docelowe rozwiązanie programowo-sprzętowe w ramach dostawy infrastruktury.

Rozdział 10 – opisuje oczekiwany sposób realizacji usługi instalacji i konfiguracji (w tym migracji danych).

Rozdział 11 - opisuje kontekst utrzymania infrastruktury sprzętowo-programowej oraz jej zagadnienia realizacyjne.

Rozdział 12 - opisuje zakres świadczenia usługi utrzymania.

Rozdział 13 – opisuje narzędzia monitoringu.

Rozdział 14 - opisuje wymagania dotyczące poziomu świadczenia usługi utrzymania.

Rozdział 15 – opisuje zasady raportowania realizacji przedmiotu zamówienia.

Rozdział 16 – opisuje oczekiwany sposób realizacji usługi asysty technicznej.

Rozdział 17 - opisuje zakres dokumentacji, która musi powstać w ramach realizacji niniejszego postępowania.

Rozdział 18 – opisuje sposób odbioru dokumentacji i raportów miesięcznych

Rozdział 19 – opisuje zakres warsztatów do realizacji.

Rozdział 20 – opisuje rolę Rady Architektury SIG.

Rozdział 21 – opisuje dodatkowe zobowiązania Wykonawcy

Rozdział 22 – opisuje dodatkowe zobowiązania Zamawiającego

Rozdział 23 – zawiera listę załączników do niniejszego dokumentu.

2 Słownik pojęć

Terminy i skróty ogólne	
BDOO	Baza Danych Obiektów Ogólnogeograficznych o szczegółowości odpowiadającej mapie ogólnogeograficznej w skali 1: 250 000 – Magazyn danych KSZBDOT.
BDOT10k	Baza danych obiektów topograficznych o szczegółowości odpowiadającej mapie topograficznej w skali 1: 10 000 - Magazyn danych KSZBDOT.
BGP	ang. Border Gateway Protocol.
CAPAP	Centrum Analiz Przestrzennych Administracji Publicznej.
Cloud Computing	Model przetwarzania w chmurze obliczeniowej.
CODGiK	Centralny Ośrodek Dokumentacji Geodezyjnej i Kartograficznej.
Czas obsługi	Maksymalny czas, liczony od momentu poprawnego zgłoszenia do momentu przekazania, przez Wykonawcę, rozwiązania i potwierdzenia przez Zamawiającego możliwości zamknięcia zgłoszenia.
Czas reakcji	Czas liczony od momentu pozyskania informacji o zdarzeniu (Incydent, zgłoszenie) do powiadomienia zgłaszającego o sposobie i terminie realizacji zdarzenia lub do momentu eskalacji tego zdarzenia.
Dyrektywa INSPIRE	Dyrektywa 2007/2/WE Parlamentu Europejskiego i Rady z dnia 14 marca 2007 r. ustanawiająca infrastrukturę informacji przestrzennej we Wspólnocie Europejskiej (INSPIRE).
Dzień roboczy	8 godzin roboczych w ramach Godzin pracy CODGiK.
dostosowania pomieszczeń serwerowni	Działanie realizowane po stronie Zamawiającego polegające na budowie wyposażeniu w niezbędną infrastrukturę pomieszczenia serwerowni w budynku CODGiK ul. Jana Olbrachta 94B, 01-102 Warszawa.
EMUiA	Ewidencja Miejscowości, Ulic i Adresów.
enviDMS	Projekt model bazy danych przestrzennych dotyczących środowiska przyrodniczego wraz z systemem zarządzania w aspekcie kartograficznych opracowań tematycznych.
e-PUAP	Elektroniczna Platforma Usług Administracji Publicznej – portal internetowy udostępniający informacje na temat usług publicznych realizowanych drogą elektroniczną.

Terminy i skróty ogólne	
GBDOT	Projekt „Georeferencyjna Baza Danych Obiektów Topograficznych (GBDOT) wraz z krajowym systemem zarządzania" realizowany w ramach Programu Operacyjnego Innowacyjna Gospodarka, lata 2007-2013, Priorytet VII Społeczeństwo informacyjne – Budowa elektronicznej administracji.
Geoportal	Portal internetowy zgodny z dyrektywą INSPIRE, pełniący rolę brokera, udostępniającego użytkownikom dane i usługi geoprzestrzenne poprzez wyszukanie żądanych informacji, którego dysponentem jest Główny Geodeta Kraju. Rozwijany w ramach projektu Geoportal2. System GEOPORTAL wraz z Systemami dziedzinowymi.
GEOPORTAL 2	Projekt rozwoju infrastruktury informacji przestrzennej w Polsce, realizowany w ramach Programu Operacyjnego Innowacyjna Gospodarka, lata 2007-2013, Priorytet VII Społeczeństwo informacyjne – Budowa elektronicznej administracji. Projekt stanowi kontynuację projektu Geoportal.gov.pl.
Godzina robocza	Okres trwający godzinę zegarową w ramach Godzin pracy Zamawiającego.
Godziny pracy CODGiK	Od 7.15 do 15.15, od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy i dni wolnych w CODGiK, o których Zamawiający poinformował Wykonawcę.
Godziny pracy Zamawiającego	Od 8.15 do 16.15, od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy i dni wolnych u Zamawiającego, o których Zamawiający poinformował Wykonawcę.
GUGiK	Główny Urząd Geodezji i Kartografii.
HSM	z ang. hardware security module, urządzenie stanowiące element infrastruktury PKI posiadające sprzętowe zabezpieczenia oraz certyfikat świadczący o klasie bezpieczeństwa.
IIP	Infrastruktura Informacji Przestrzennej.
Incydent	Nieplanowana przerwa lub obniżenie jakości usługi biznesowej.
Incydent standardowy	Każdy inny nie będący Incydentem pilnym ani Incydentem krytycznym.
Incydent krytyczny	Incydent uniemożliwiający korzystanie z usług biznesowych w co najmniej jednej lokalizacji.
Incydent pilny	Incydent uniemożliwiający korzystanie z usług biznesowych na co najmniej jednym stanowisku w lokalizacji.
IPE	Integrująca Platforma Elektroniczna

Terminy i skróty ogólne	
ISOK	Projekt ISOK (Informatyczny System Osłony Kraju przed nadzwyczajnymi zagrożeniami) realizowany przez konsorcjum Krajowy Zarząd Gospodarki Wodnej, Instytut Meteorologii i Gospodarki Wodnej, Główny Urząd Geodezji i Kartografii, Rządowe Centrum Bezpieczeństwa i Instytut Łączności.
ITIL	Kodeks postępowania dla działów informatyki, zawierający zbiór zaleceń jak efektywnie i skutecznie oferować usługi informatyczne.
KSZBDOT	Krajowy System Zarządzania Bazą Danych Obiektów Topograficznych.
NMPT	Numeryczny Model Pokrycia Terenu.
NMT	Numeryczny Model Terenu.
Oprogramowanie standardowe	Gotowe oprogramowanie publicznie dostępne w sprzedaży, stanowiące dla organizacji alternatywny sposób pozyskania poza samodzielnym ich wytworzeniem. Oprogramowanie Standardowe jest produktem typu COTS (Commercial Off-The-Shelf).
OPZ	Opis przedmiotu zamówienia.
POPC	Program Operacyjny Polska Cyfrowa.
PRINCE 2	Metodyka zarządzania projektami. Właścicielem metodyki jest Office Government Commerce.
PRNG	Państwowy Rejestr Nazw Geograficznych.
Problem	Przyczyna jednego lub wielu Incydentów.
Pryncypia Architektury Korporacyjnej	Materiał opracowany w ramach Zespołu do spraw rozwoju strategii informatyzacji administracji publicznej w Ministerstwie Administracji i Cyfryzacji https://mac.gov.pl/projekty/architektura-korporacyjna-panstwa.
PZGiK	Państwowy Zasób Geodezyjny i Kartograficzny.
RCiWN	Rejestr Cen i Wartości Nieruchomości.
RPO	(ang. recovery point objective) – akceptowalny poziom utraty danych wyrażony w czasie
RTO	(ang. recovery time objective) – czas w jakim należy przywrócić proces po wystąpieniu awarii
SCMIS	(ang. supplier and contract management information system) System Zarządzania Dostawcami i Umowami

Terminy i skróty ogólne	
SIG	Systemy Informatyczne GUGiK - Zestaw metod, narzędzi i wytycznych dotyczących realizacji projektów w Głównym Urzędzie Geodezji i Kartografii. W szczególności są to systemy informatyczne działające w infrastrukturze sprzętowo programowej Zamawiającego oraz w odniesieniu do przyszłości także systemy i narzędzia planowane do budowy i wdrożenia.
SIWZ	Specyfikacja Istotnych Warunków Zamówienia.
SSO	ang. Single Sign On. Szczególna forma uwierzytelnienia pozwalająca użytkownikowi uwierzytelnić się tylko raz i uzyskać dostęp do zasobów wielu systemów, do których nadano użytkownikowi uprawnienia.
Strony	Zamawiający i Wykonawca.
SZBI	System Zarządzania Bezpieczeństwem Informacji.
SZNMT	System Zarządzania Numerycznym Modelem Terenu.
TERYT 2	Projekt TERYT 2 - Państwowy rejestr granic i powierzchni jednostek podziałów terytorialnych kraju realizowany w ramach Programu Operacyjnego Innowacyjna Gospodarka, lata 2007-2013, Priorytet VII Społeczeństwo informacyjne – Budowa elektronicznej administracji.
TERYT 3	Projekt TERYT 3 - Rozbudowa systemów do prowadzenia rejestrów adresowych – Etap I, realizowany w ramach Programu Operacyjnego Innowacyjna Gospodarka, lata 2007-2013, Priorytet VII Społeczeństwo informacyjne – Budowa elektronicznej administracji.
UE	Unia Europejska.
UMM	Uniwersalny Moduł Mapowy.
Umowa	Umowa, która zostanie podpisana na realizację Zamówienia.
Usługi Asysty	Wsparcie Zamawiającego przez Wykonawcę. Szczegółowy zakres wsparcia będzie określony w chwili wystąpienia takiej potrzeby i może dotyczyć rozwoju systemu, np. dodawania nowych funkcjonalności lub modyfikacji aktualnego systemu.
Ustawa IIP/Ustawa o IIP	Ustawa o Infrastrukturze Informacji Przestrzennej (Dz .U. nr 76, poz. 489) z 4 marca 2010r.
Ustawa PGiK, PGiK	Ustawa z dnia 17 maja 1989 r. - Prawo geodezyjne i kartograficzne (Dz.U. 2010, nr 193 poz. 1287).
WMS	Web Map Service (WMS) to międzynarodowy standard udostępniania danych przestrzennych w Internecie w postaci rastrowej. Standardy techniczne dostępne są na stronie Open Geospatial Consortium (OGC).

Terminy i skróty ogólne	
WMTS	Web Map Tile Service (WMTS) to międzynarodowy standard udostępniania danych przestrzennych w Internecie w postaci rastrowych, predefiniowanych fragmentów mapy tzw. kafli. Proces generowania kafli jest uruchamiany po aktualizacji danego produktu natomiast pliki zapisywane są na serwerach w odpowiedniej strukturze. Zastosowanie takiego rozwiązania przyspiesza odpowiedź usługi na zapytanie użytkownika o fragment mapy ponieważ zwracana jest już wcześniej przygotowana grafika w przeciwieństwie do usługi WMS, która generuje plik graficzny każdorazowo po otrzymaniu takiego zlecenia.
WODGiK	Wojewódzki Ośrodek Dokumentacji Geodezyjnej i Kartograficznej.
Wykonawca	Podmiot, który zawrze z Zamawiającym umowę sprawie wykonania Zamówienia.
Wykonawca rozwoju i budowy usług	Podmiot, który będzie realizował zadania związane z rozwojem systemów SIG w ramach działania budowy i udostępniania usług w ramach Projektów CAPAP, ZSIN Faza II i K-GESUT, współfinansowanych ze środków Programu Operacyjnego Polska Cyfrowa Oś 2 Działanie 2.1 „Wysoka dostępność i jakość e-usług publicznych”.
Wykonawca systemów	Podmiot, który będzie realizował zadania związane z rozwojem systemów SIG w ramach działania budowy i udostępniania usług w ramach Projektów CAPAP, ZSIN Faza II i K-GESUT, współfinansowanych ze środków Programu Operacyjnego Polska Cyfrowa Oś 2 Działanie 2.1 „Wysoka dostępność i jakość e-usług publicznych”.
Zamawiający	Główny Urząd Geodezji i Kartografii.
Zamówienie	Zamówienie publiczne, którego przedmiot w sposób szczegółowy został opisany w SOPZ.
Zgłoszenie standardowe	Dowolna prośba użytkownika o informację, konsultację, poradę, standardową zmianę lub nadanie dostępu do usługi / aplikacji.
Zintegrowany moduł mapowy PZGiK	Produkty powstające w ramach narzędzi do udostępniania danych, dedykowane dla poszczególnych branż i grup odbiorców. Zintegrowane moduły mapowe będą udostępniać dane, usługi i analizy najbardziej istotne i najbardziej adekwatne dla potrzeb przedstawicieli danej branży.
ZSIN	Zintegrowany System Informacji o Nieruchomościach.

3 Podstawowe informacje o projektach

Zamówienie dotyczące budowy i udostępniania usług będzie realizowane w ramach Projektów CAPAP, ZSIN Faza II i K-GESUT, współfinansowanych ze środków Programu Operacyjnego Polska Cyfrowa Oś 2 Działanie 2.1 „Wysoka dostępność i jakość e-usług publicznych".

3.1 Projekt CAPAP

Głównym celem strategicznym CAPAP jest zwiększenie stopnia wykorzystania danych przestrzennych przez obywateli, przedsiębiorców i administrację publiczną.

Projekt CAPAP stanowi naturalną kontynuację działań realizowanych wcześniej przez GUGiK, w ramach których powstały narzędzia umożliwiające wypełnienie zapisów INSPIRE m.in. w zakresie tworzenia i udostępniania brokerów usług, a także zadań, w ramach których wytwarzane były dane dziedzinowe dla tematów INSPIRE oraz budowane i rozbudowywane były systemy informatyczne do zarządzania tymi danymi.

Według przyjętych założeń Centrum Analiz Przestrzennych Administracji Publicznej będzie wspólnym dla administracji publicznej środowiskiem kompetencyjno-analitycznym, które umożliwi udostępnianie zaawansowanych usług związanych z informacją przestrzenną.

Usługi CAPAP świadczone będą obywatelom, przedsiębiorcom oraz administracji publicznej i związane będą z informacją przestrzenną pochodzącą z rejestrów georeferencyjnych, istotnych między innymi dla prowadzenia działalności gospodarczej, zrównoważonego rozwoju, ochrony środowiska, zarządzania.

Poza ww. usługami zakłada się udostępnienie innowacyjnych usług elektronicznych (e-usług) wytworzonych w oparciu o zintegrowane dane państwowego zasobu geodezyjnego i kartograficznego (PZGiK) i dane geoprzestrzenne administracji rządowej i samorządowej oraz zapewnienie efektywnego dostępu do przetworzonej zgodnie z potrzebami użytkowników informacji geoprzestrzennej.

3.2 Projekt ZSIN

Głównym celem strategicznym Projektu ZSIN – Faza II jest zwiększenie efektywności pracy urzędów w zakresie rejestrów związanych z nieruchomościami oraz podniesienie poziomu obsługi obywateli i przedsiębiorców w zakresie działań związanych z pozyskiwaniem informacji o nieruchomościach.

Projekt ZSIN – Budowa Zintegrowanego Systemu Informacji o Nieruchomościach – Faza II (Projekt ZSIN – Faza II) stanowi kontynuację Projektu ZSIN – Faza I realizowanego w ramach 7. osi POIG.

Projekt umożliwi usprawnienie wielu procesów realizowanych zarówno przez administrację publiczną jak i wybrane podmioty wykorzystujące informacje o nieruchomościach.

Projekt cechuje złożony charakter tworzonego systemu, dużą liczbę podmiotów zaangażowanych w jego tworzenie, a także zróżnicowany stan danych utrzymywanych w rejestrach objętych Projektem.

Prawny obowiązek realizacji Projektu wynika z ustawy z dnia 17 maja 1989 r. Prawo geodezyjne i kartograficzne, oraz rozporządzenia Rady Ministrów z dnia 17 stycznia 2013 r. w sprawie zintegrowanego systemu informacji o nieruchomościach. Jako członek UE Polska jest zobowiązana do wdrażania Dyrektywy 2007/2/WE Parlamentu Europejskiego i Rady z dnia 14 marca 2007 r. ustanawiającej infrastrukturę informacji przestrzennej we Wspólnocie Europejskiej (INSPIRE).

3.3 Projekt K-GESUT

Celem strategicznym projektu K-GESUT jest zwiększenie stopnia wykorzystania potencjału danych w zakresie sieci uzbrojenia terenu przez administrację publiczną, przedsiębiorców i obywateli.

Idea realizacji projektu powstała w związku z wejściem w życie Ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych (Dz. U. Nr 106, poz. 675 z późn. zm.), która poprzez art. 29 ust. 4 nakłada na Głównego Geodetę Kraju obowiązek udostępniania informacji z centralnej części państwowego zasobu geodezyjnego i kartograficznego, niezbędnych dla potrzeb wykonania przez Prezesa UKE inwentaryzacji zawierającej pokrycie istniejącą infrastrukturą i publicznymi sieciami telekomunikacyjnymi zapewniającymi lub umożliwiającymi zapewnienie szerokopasmowego dostępu do Internetu.

Przywołana powyżej Ustawa znowelizowała Ustawę PGiK, poprzez dodanie art. 7a ust. 1 pkt 16a, który narzuca na Głównego Geodetę Kraju obowiązek założenia i prowadzenia krajowej bazy GESUT.

Ponadto, zgodnie z projektem założeń Ustawy o zmianie ustawy o wspieraniu rozwoju usług i sieci telekomunikacyjnych oraz niektórych innych ustaw, która stanowi implementację do polskiego porządku prawnego Dyrektywy kosztowej, krajowa baza GESUT stanowić będzie rejestr źródłowy do pozyskania informacji o sieciach uzbrojenia terenu, celem utworzenia pojedynczego punktu informacyjnego. Zadaniem tego punktu będzie m. in. koordynacja robót budowlanych dotyczących infrastruktury technicznej, w tym sieci uzbrojenia terenu oraz współdzielenie kosztów inwestycyjnych.

Realizacja projektu w sposób pośredni wynika również z prawnych zobowiązań wobec UE, a mianowicie z postanowień Dyrektywy INSPIRE. Transpozycja Dyrektywy INSPIRE do polskiego porządku prawnego została dokonana poprzez Ustawę o IIP.
Krajowa baza GESUT, której proces tworzenia zostanie wsparty poprzez szereg działań realizowanych w ramach projektu, stanowić będzie bazę źródłową do zasilenia tematu danych przestrzennych „usługi użyteczności publicznej i służby państwowe", o którym mowa w załączniku do ww. Ustawy i dla którego organem wiodącym jest Główny Geodeta Kraju. Baza ta stanowić będzie bazę źródłową do zasilenia przedmiotowego tematu danych przestrzennych w zakresie instalacji użyteczności publicznej w szczególności (kanalizacja, dostawa energii i dostawa wody).

W związku z powyższym oraz z uwagi na brak spójnej, aktualnej i zharmonizowanej informacji przestrzennej o sieciach uzbrojenia terenu, podjęto działania zmierzające do założenia krajowej bazy GESUT, którą z zgodnie z art. 28a Ustawy PGiK tworzy się przede wszystkim na podstawie powiatowych baz GESUT.

W ramach podjętych działań w 2012 r. zbudowano system zarządzania krajową bazą GESUT, który zakłada tworzenie i aktualizację krajowej bazy GESUT.
Jednakże, z uwagi na niedostosowanie danych powiatowej bazy GESUT do przyjętego modelu danych, proces tworzenia i aktualizacji krajowej bazy GESUT jest procesem mało efektywnym w stosunku do zidentyfikowanych potrzeb odbiorców.

Zatem, utworzenie informacji przestrzennej o sieciach uzbrojenia terenu w postaci krajowej bazy GESUT wymaga usprawnienia procesów organizacyjnych, technicznych oraz technologicznych. Ich usprawnienie wpłynie na poprawę jakości i wiarygodności danych dotyczących sieci uzbrojenia terenu, obniżenie kosztów ich prowadzenia oraz podniesienia poziomu obsługi obywateli i przedsiębiorców. Poprzez nowe usługi zaplanowane do realizacji w projekcie zwiększona zostanie dostępność do zbiorów danych przestrzennych i metadanych pozostających w dyspozycji administracji publicznej. Harmonizacja rejestrów publicznych prowadzonych w systemach teleinformatycznych pozytywnie wpłynie na jakość danych przestrzennych oraz zwiększenie ich interoperacyjności.

Obecnie dane przestrzenne o sieciach uzbrojenia terenu są przechowywane w sposób rozproszony terytorialnie, z wykorzystaniem różnych technologii (w znacznej mierze w formie nieelektronicznej) oraz różnych aplikacji. W konsekwencji możliwości wglądu do tych danych są ograniczone i niejednorodne. Tymczasem informacje o sieciach uzbrojenia terenu są wymagane przy realizacji szeregu działań podejmowanych przez obywateli, przedsiębiorców oraz administrację. W szczególności dane takie powinny być dostępne podczas planowania strategicznego, planowania

czy lokalizowania inwestycji. Niemniej ważne są potrzeby służb ratunkowych, dla których istotna jest informacja o sieciach uzbrojenia terenu na miejscu planowanej i realizowanej akcji. Planowane przedsięwzięcie ma odpowiadać na te potrzeby. Ponadto, w sposób pośredni wspierając działania administracji i służb ratunkowych, projekt odpowiada na potrzebę podniesienia poziomu bezpieczeństwa oraz dobrego zarządzania państwem.

4 Opis organizacji zamówienia

Główny Urząd Geodezji i Kartografii (GUGiK) jest urzędem obsługującym Głównego Geodetę Kraju, który wykonuje zadania określone w szczególności w Ustawie Prawo Geodezyjne i Kartograficzne, Ustawie o Infrastrukturze Informacji Przestrzennej. GUGiK realizuje szereg projektów, w ramach których powstają systemy informatyczne.

Centralny Ośrodek Dokumentacji Geodezyjnej i Kartograficznej (CODGiK) jest instytucją gospodarki budżetowej. Przedmiotem działalności podstawowej CODGiK jest wykonywanie czynności materialno-technicznych służących realizacji zadań publicznych przypisanych Głównemu Geodecie Kraju, m.in. w zakresie:

- baz danych i systemów zarządzania centralnego zasobu geodezyjnego i kartograficznego;
- utrzymania serwerów katalogowych i serwerów metadanych;
- tworzenia i obsługi usług sieciowych dotyczących zbiorów i usług danych przestrzennych,
- interoperacyjności zbiorów i usług danych przestrzennych;
- wdrażania i utrzymywania rozwiązań technicznych zapewniających określoną przepisami wydajność i dostępność serwisów geoportalu infrastruktury informacji przestrzennej;
- dostępności i ciągłości działania systemów teleinformatycznych;
- bezpieczeństwa systemów i sieci teleinformatycznych.

Ponadto CODGiK bierze m.in. czynny udział w procesie utrzymania rezultatów projektów zrealizowanych przez GUGiK w ramach 7 osi priorytetowej „Społeczeństwo informacyjne – budowa elektronicznej administracji" Programu Operacyjnego Innowacyjna Gospodarka, 2007 – 2013, w szczególności projektu GEOPORTAL 2.

Projekt, rozumiany jako realizacja przedmiotowej Umowy, musi być realizowany zgodnie z metodyką zarządzania projektami PRINCE2.

W odniesieniu do metodyki PRINCE2, niniejsze zamówienie będzie realizowane, jako Grupa Zadań wykonywana w ramach projektu.

Zakres odpowiedzialności i uprawnień dla poszczególnych ról projektowych należy rozumieć zgodnie z zaleceniami metodyki PRINCE2. W odniesieniu do tej metodyki kierownik projektu niniejszego postępowania po stronie Wykonawcy rozumiany będzie, jako kierownik grupy zadań, podlegający bezpośrednio kierownikowi Projektu ze strony Zamawiającego.

Wykonawca zobowiązany będzie realizować swoje prace głównie w siedzibie Centralnego Ośrodka Dokumentacji Geodezyjnej i Kartograficznej, ul. Jana Olbrachta 94 B w Warszawie oraz dodatkowo w Głównym Urzędzie Geodezji i Kartografii, Centrum Zarządzania ASG-EUPOS w Katowicach, ul. Graniczna 29, 40-017 Katowice.

Raport z wykonania usług Wykonawcy, będący podstawą rozliczeń prac Wykonawcy, weryfikowany będzie przez Zamawiającego (Główny Urząd Geodezji i Kartografii), w porozumieniu z Centralnym Ośrodkiem Dokumentacji Geodezyjnej i Kartograficznej.

4.1 Struktura organizacyjna

Projekty CAPAP, ZSIN - Faza II i K-GESUT są realizowane zgodnie z metodyką zarządzania projektami PRINCE2. Metodyka PRINCE 2 została wdrożona i była wykorzystywana przez Główny Urząd Geodezji i Kartografii przy realizacji wszystkich projektów w ramach Programu Operacyjnego Innowacyjna Gospodarka, w tym:

1) GEOPORTAL.GOV.PL
   Cel projektu:
   - uruchomienie portalu internetowego udostępniającego dane i usługi geoprzestrzenne oraz przetworzenie wybranych opracowań geodezyjnych i kartograficznych do postaci numerycznej.

   Termin zakończenia realizacji: październik 2008 r.
2) TERYT 2 - Państwowy rejestr granic i powierzchni jednostek podziałów terytorialnych kraju
   Cel projektu:
   - udostępnienie on-line Państwowego Rejestru Granic i Powierzchni Jednostek Podziałów Terytorialnych Kraju oraz realizacja i wdrożenie rozwiązań związanych z prowadzeniem rejestrów adresowych.

   Termin zakończenia projektu: grudzień 2012 r.
3) GEOPORTAL 2 - Rozbudowa infrastruktury informacji przestrzennej w zakresie rejestrów georeferencyjnych oraz związanych z nimi usług.
   Cel projektu:
   - umożliwienie powszechnego dostępu i stosowania informacji przestrzennej w Polsce poprzez rozbudowę infrastruktury informacji przestrzennej w zakresie rejestrów georeferencyjnych oraz związanych z nimi usług.

   Termin zakończenia projektu: grudzień 2015 r.
4) GBDOT - Georeferencyjna Baza Danych Obiektów Topograficznych (GBDOT) wraz z krajowym systemem zarządzania.
   Cel projektu:
   - Budowa zharmonizowanej bazy danych zawierającej informacje o lokalizacji obiektów przestrzennych i zjawisk na obszarze całego kraju, w szczególności w zakresie bazy danych obiektów topograficznych (BDOT10k) i bazy danych obiektów

ogólnogeograficznych (BDOO), zawierających informacje o obiektach topograficznych z kategorii tj.:

- Sieć wodna;
- Sieć komunikacyjna (drogi i koleje);
- Sieć uzbrojenia terenu;
- Kompleksy pokrycia terenu;
- Budynki, budowle i urządzenia; ;
- Kompleksy użytkowania terenu;
- Inne obiekty przestrzenne.

- Budowa Krajowego Systemu Zarządzania Bazą Danych Obiektów Topograficznych wraz z centrum zapasowym.

Termin zakończenia projektu: listopad 2015 r.

5) ISOK - Informatyczny System Osłony Kraju przed nadzwyczajnymi zagrożeniami.
Projekt był realizowany w ramach konsorcjum w skład którego wchodzą:
   - Krajowy Zarząd Gospodarki Wodnej (lider konsorcjum).
   - Instytut Meteorologii i Gospodarki Wodnej;
   - Główny Urząd Geodezji i Kartografii;
   - Instytut Łączności;

   Cel projektu:
   - stworzenie systemu osłony społeczeństwa, gospodarki i środowiska przed nadzwyczajnymi zagrożeniami poprzez stworzenie elektronicznej platformy informatycznej wraz z niezbędnymi rejestrami referencyjnymi, która stanowić będzie narzędzie do zarządzania kryzysowego.

   Główny cel projektu w zakresie realizowanym przez Główny Urząd Geodezji i Kartografii:
   - budowa referencyjnych, zharmonizowanych i interoperacyjnych baz danych przestrzennych do których docelowo dostęp będzie możliwy dzięki usługom uruchamianym w ramach realizacji projektu GEOPORTAL 2.

   Termin zakończenia projektu: grudzień 2015 r.
6) TERYT 3 – Rozbudowa systemów do prowadzenia rejestrów adresowych – Etap I.
   Cel projektu:
   - zapewnienie obywatelom, przedsiębiorcom i organom administracji publicznej dostępu przy pomocy środków komunikacji elektronicznej do kompletnych, wiarygodnych i aktualnych danych z rejestrów adresowych (w tym również obejmujących lokalizację przestrzenną).

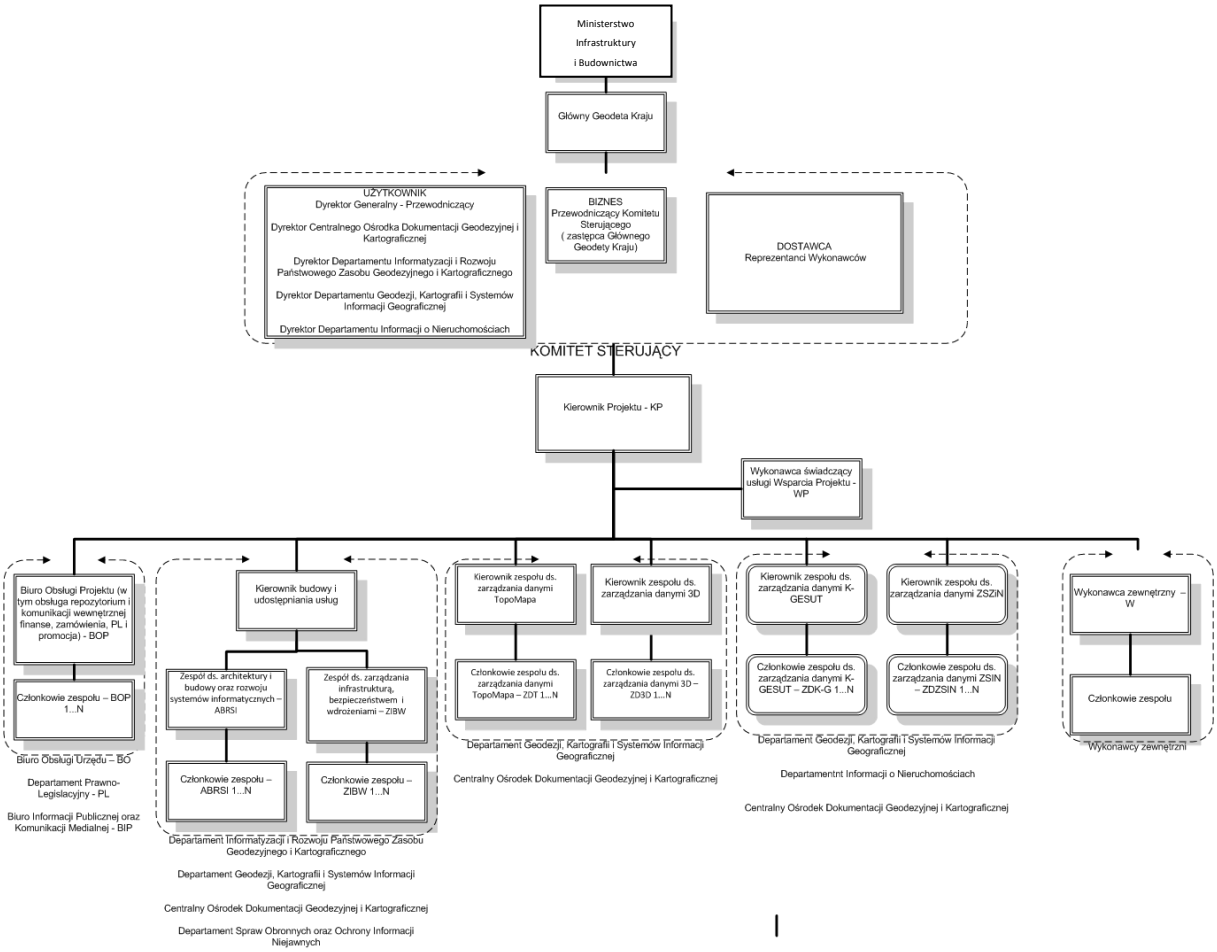
   Termin zakończenia projektu: grudzień 2015 r.
7) ZSIN – Budowa Zintegrowanego Systemu Informacji o Nieruchomościach – Faza I.
   Cel projektu:
   - usprawnienie procesu obsługi spraw prowadzonych przez administrację publiczną
   - w zakresie rejestracji nieruchomości oraz zapewnienia obywatelom i przedsiębiorcom dostępu do wiarygodnych i aktualnych informacji o nieruchomościach gromadzonych w rejestrach publicznych.

   Termin zakończenia projektu: grudzień 2015 r.

Z uwagi na wieloletnie doświadczenia Zamawiającego związane ze stosowaniem metodyki PRINCE2, metodyka zastosowana w ramach realizacji POPC będzie opierała się również o dotychczasowe doświadczenia z jej stosowania.

Na poniższym rysunku przedstawiona została struktura organizacyjna zarządzania projektem.

Rysunek 1 Struktura organizacyjna



Zakres odpowiedzialności i uprawnień dla poszczególnych ról projektowych należy rozumieć zgodnie z zaleceniami metodyki PRINCE2. W odniesieniu do tej metodyki kierownik projektu niniejszego postępowania po stronie Wykonawcy rozumiany będzie, jako kierownik grupy zadań, podlegający bezpośrednio kierownikom projektów CAPAP, ZSIN-Faza II i K-GESUT (po stronie Zamawiającego).

Wykonawca zobowiązany będzie do realizacji działań zarządczych (m.in. zarządzanie ryzykiem, zarządzanie zagadnieniami, zarządzanie komunikacją) zgodnie z wytycznymi, które zostaną przekazane przez Zamawiającego po podpisaniu Umowy. Wytyczne będą zawierać w szczególności procedury postępowania (np. procedura zgłaszania ryzyka) oraz zasady dla obszaru zarządczego (np. klasyfikacja ryzyk projektowych, wzory Rejestrów), które zostały ustanowione dla projektu.

4.2 SIG

W ramach Głównego Urzędu Geodezji i Kartografii powstała inicjatywa SIG - inicjatywa mająca na celu wypracowanie i wdrożenie spójnego systemu zasad działania dla wszystkich inicjatyw/projektów realizowanych przez Główny Urząd Geodezji i Kartografii. Inicjatywa powstała w wyniku dostrzeżenia potrzeby zarządzania wszystkimi przedsięwzięciami realizowanymi przez Główny Urząd Geodezji i Kartografii, których rezultatami jest dostarczenie rozwiązań informatycznych wspierających realizację zadań Głównego Urzędu Geodezji i Kartografii. Inicjatywa SIG swoim zakresem wpływa na sposób realizacji projektów CAPAP, ZSIN - Faza II i K-GESUT, gdyż dostarcza wewnętrznych standardów i wytycznych, a także dobrych praktyk wypracowanych w oparciu o doświadczenia ze zrealizowanych projektów.

Inicjatywa ta została podzielona na 3 główne obszary:

- obszar architektury, którego celem jest zapewnienie spójności budowanych rozwiązań na poziomie systemów informatycznych;
- obszar realizacji, którego celem jest zapewnienie spójnej realizacji projektów/przedsięwzięć;
- obszar utrzymania, którego celem jest zapewnienie jednolitego sposobu utrzymania wyników projektów/przedsięwzięć.

W ramach zapewniania **spójnej architektury rozwiązania** SIG realizowane są następujące działania z obszarów:

- integracji warstwy biznesowej, w ramach której powstały:
    - jednolity katalog usług biznesowych planowanych/udostępnianych w ramach projektów/przedsięwzięć;
    - mapa usług biznesowych przedstawiająca powiązania pomiędzy usługami biznesowymi;
    - mapa produktów dostarczanych w ramach projektów/przedsięwzięć wraz z powiązaniami pomiędzy nimi;
    - standardy jednolitej dokumentacji;
    - pryncypia architektoniczne;
    - Rada Architektury i Biuro Architektury rozwiązująca zagadnienia dot. integracji systemów informatycznych;
- integracji warstwy IT, w ramach której powstały:
    - wytyczne i standardy dotyczące integracji pomiędzy systemami i dotyczące reużywalności poszczególnych komponentów;

  - model statyczny SIG przedstawiający architekturę rozwiązań;
  - scenariusze integracji dla systemów informatycznych;
  - ujednolicone modele wymagań;
  - diagram przepływu danych;
  - metoda wymiarowania usług na potrzeby szacowania zapotrzebowania na infrastrukturę;
- infrastruktury, uwzględniającej optymalne wykorzystanie istniejącej infrastruktury.

Architektura rozwiązania została opracowana w taki sposób, aby zapewnić możliwość dostosowania wdrażanych rozwiązań do nowych wytycznych cyfryzacji, w sposób optymalny pod względem kosztów i czasu.

Jednolity sposób realizacji inicjatyw w ramach SIG obejmuje:

- realizację w oparciu o wytyczne metodyki PRINCE2;
- stosowania zbioru wytycznych w obszarach zarządzania jakością, konfiguracją, ryzykiem i komunikacją;
- wsparcie narzędziowe w obszarze organizacji, architektury i utrzymania.

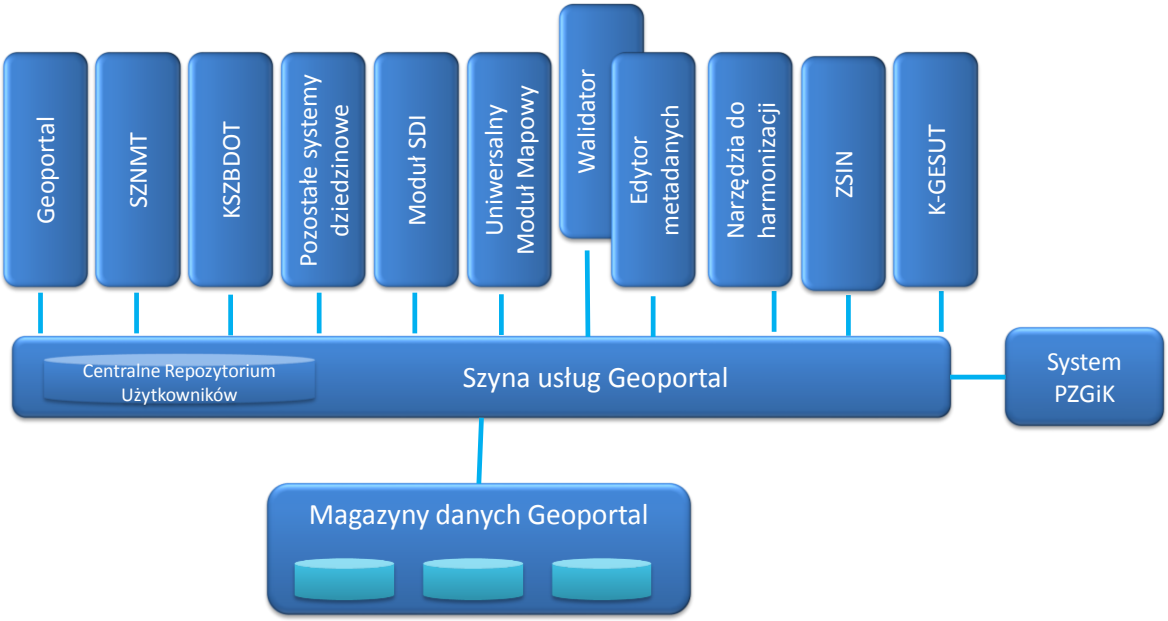
Jednolity sposób utrzymania SIG osiągnięty został poprzez:

- stworzenie spójnego modelu utrzymania bazującego na dobrych praktykach ITIL;
- świadczenie usług biznesowych na ustalonych parametrach;
- zapewnienie mechanizmów organizacyjnych i technicznych ciągłego monitorowania.

Inicjatywa SIG objęła swoim zasięgiem znaczącą większość systemów informatycznych, które były wytwarzane i dostarczane dla GUGiK. Systemy informatyczne istotne z perspektywy Projektów CAPAP, ZSIN - Faza II i K-GESUT opisane zostały w poniższych podrozdziałach.

Architekturę logiczną SIG przedstawia Rysunek 2 Architektura logiczna SIG.

Rysunek 2 Architektura logiczna SIG



Podstawowym elementem architektury SIG jest szyna usług, która zapewnia komunikację pomiędzy Systemem Geoportal, poszczególnymi systemami dziedzinowymi, pozostałymi systemami i aplikacjami (m.in. Systemem PZGiK, Modułem SDI, Uniwersalnym Modułem Mapowym, a także narzędziami do zarządzania metadanymi – Edytorem i Walidatorem metadanych oraz narzędziami do harmonizacji). System Geoportal dodatkowo korzysta z Magazynów danych Geoportal stanowiących replikę publikacyjną danych dziedzinowych, które produkowane są za pomocą systemów dziedzinowych (magazyny produkcyjne systemów dziedzinowych oraz magazyny pomocnicze Modułu SDI, UMM i narzędzi do zarządzania metadanymi).

Opis poszczególnych komponentów architektury SIG znajduje się w poniższych podrozdziałach.

Zamawiający posiada dokumentację poszczególnych komponentów. Dokumentacja zostanie udostępniona Wykonawcy po zawarciu umowy.

W rozdziale 6. Opis techniczny systemów SIG przedstawione zostały informacje dotyczące technologii zastosowanej w systemach informatycznych GUGiK.

5 Przedmiot zamówienia

Przedmiotem Zamówienia jest

1. Dostawa infrastruktury sprzętowej do środowiska SIG oraz oprogramowania, wraz z udzieleniem nieograniczonej w czasie licencji, opisanej w rozdziale 9. Dostawa infrastruktury i oprogramowania**Błąd! Nie można odnaleźć źródła odwołania.**,
2. Zapewnienie usług wsparcia technicznego na dostarczone elementy infrastruktury sprzętowej oraz oprogramowanie, na okres zgodny z ofertą Wykonawcy - „Czas Trwania Wsparcia Technicznego", od daty podpisania Protokołu Odbioru Dostawy do Umowy (Szczegółowe warunki wsparcia technicznego zostały opisane w rozdziale 9 - Dostawa infrastruktury i oprogramowania),
3. Instalacja i konfiguracja dostarczonej infrastruktury sprzętowej i oprogramowania opisana w rozdziale 10. Instalacja i konfiguracja dostarczonej infrastruktury i oprogramowania.
4. Świadczenie usług utrzymania infrastruktury SIG dostarczonej w dużej części w ramach projektu GEOPORTAL 2, współfinansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka, 7 Oś priorytetowa - Społeczeństwo informacyjne – budowa elektronicznej administracji, w zakresie zgodnym z niniejszym dokumentem, oraz nowej infrastruktury (zgodnie z pkt. 1) po jej dostarczeniu, obejmujący w szczególności:
   1) Świadczenie usług utrzymania infrastruktury w zakresie i na zasadach opisanych w rozdziałach 11. Utrzymanie i 12. Zakres prac Utrzymaniowych niniejszego Szczegółowego Opisu Przedmiotu Zamówienia,
   2) Przedmiot zamówienia będzie realizowany zgodnie z najlepszymi praktykami biblioteki ITIL 2011 Edition;
5. Świadczenie usług asysty technicznej w zakresie każdorazowo ustalanym z Zamawiającym, nie wykraczającym poza obszar Zamówienia opisane w rozdziale 16. Asysta techniczna,
6. Przeprowadzenie warsztatów w zakresie opisanym w rozdziale 19 Warsztaty.

6 Opis techniczny systemów SIG

Poniżej przedstawione zostały systemy informatyczne SIG, które w chwili obecnej funkcjonują w infrastrukturze Zamawiającego.

6.1 System Geoportal

System Geoportal umożliwia łączenie zbiorów danych przestrzennych pochodzących z zasobów różnych organów państwowych w spójną całość, dostępną w formie elektronicznej poprzez punkt dostępowy (www.geoportal.gov.pl) na interaktywnej przeglądarce map z narzędziami umożliwiającymi wyszukiwanie danych przestrzennych. Przygotowane rozwiązania punktu, tworzone zgodnie z założeniami dyrektywy INSPIRE, zapewniają dostęp do danych przestrzennych i usług zgromadzonych zarówno w krajowej jak i w europejskiej infrastrukturze informacji przestrzennej.

Od strony koncepcyjnej aplikacja daje możliwość operowania pośród czterech modułów:

- Geoportalu krajowego,
- Geoportalu branżowego,
- Geoportalu INSPIRE,
- Modułu statystyk.

Każdy z nich jest jednocześnie brokerem usług charakterystycznych dla pełnionej przez siebie roli.

Geoportal/broker krajowy

Broker krajowy (krajowy geoportal) jest głównym punktem dostępowym do krajowej Infrastruktury Informacji Przestrzennej. Rola ta determinuje możliwość udostępnienia za jego pośrednictwem wszystkich usług danych przestrzennych stanowiących część krajowej Infrastruktury Informacji Przestrzennej. Analogiczna sytuacja dotyczy metadanych opisujących polskie zbiory oraz usługi danych przestrzennych, które powinny zostać udostępnione z wykorzystaniem serwera katalogowego krajowego geoportalu.

Jedną z elementarnych ról krajowego geoportalu jest możliwość przeglądania danych przestrzennych. Warstwy dostępne za pośrednictwem przeglądarki pochodzą z zasobów PZGiK m.in. z systemów dziedzinowych. Zestawienie grup tematycznych prezentowanych w geoportalu wraz z poszczególnymi warstwami:

- Państwowy Rejestr Nazw Geograficznych (miejscowości, obiekty fizjograficzne),

- Państwowy Rejestr Granic (etykiety nazw województw, powiatów i gmin, granice administracyjne województw, powiatów i gmin),
- Dane ewidencyjne i dane o charakterze katastralnym (w ramach Krajowej Infrastruktury Informacji Przestrzennej – numery działek, działki oraz budynki),
- Rzeźba terenu (produkty pochodne Numerycznego Modelu Terenu cieniowanie, hipsometria),
- Wizualizacja Bazy Danych Obiektów Ogólnogeograficznych (BDOO) o szczegółowości i treści odpowiadającej mapie ogólnogeograficznej w skali 1: 250 000,
- Wizualizacja bazy VMap L2 o szczegółowości i treści odpowiadającej wojskowej mapie topograficznej w skali 1:50 000,
- Wizualizacja Bazy Danych Obiektów Topograficznych (BDOT10k) o szczegółowości i treści odpowiadającej mapie topograficznej w skali 1:10 000,
- Ortofotomapa (aktualna i archiwalna cyfrowa ortofotomapa lotnicza pokrywająca powierzchnię całego kraju),
- Skany map topograficznych i ogólnogeograficznych w skalach 1: 10 000, 1: 25 000, 1: 50 000, 1: 100 000, 1: 250 000, 1: 500 000, 1: 1 000 000, 1: 4 000 000,
- Przeglądowa mapa Europy (granice państw).

Broker umożliwia również wyszukiwanie metadanych opisujących zbiory danych przestrzennych. Wyszukiwanie podzielono na proste polegające na wyszukiwaniu na podstawie słów kluczowych oraz zaawansowane, uwzględniające w operacji: zawieranie się zbioru w aktualnie wyświetlanym zasięgu mapy, typ zasobu (zbiór danych, seria zbiorów danych, usługa, wszystkie), kategoryzację (kategoria tematyczna, słowa kluczowe, temat danych przestrzennych, układ współrzędnych) oraz ograniczenia w publicznym dostępie do zbiorów oraz w warunkach dostępu i korzystania. Broker umożliwia również rozproszone wyszukiwanie metadanych pochodzących z innych serwerów katalogowych IIP.

Efektem opisanego wyżej procesu wyszukiwania metadanych jest możliwość przeglądania wyników spełniających zadane kryteria. Wyniki prezentowane są w postaci listy metadanych, z której możliwe jest przejście do opisu poszczególnych zbiorów (serii, usług) danych przestrzennych. Metadane zgrupowane są w zakładkach (opis, kwalifikacja, ograniczenia, jakość, metadane), co umożliwia przyjazne zapoznanie się z ich zawartością. Ponadto możliwe jest również wyświetlenie zasięgu przestrzennego zbioru danych opisanego wyszukanymi metadanymi, przybliżenie widoku mapy do tego zasięgu oraz wyświetlenie warstw usług przeglądania wyszukanych zbiorów danych.

Geoportal/broker branżowy

Broker branżowy jest nowatorskim rozwiązaniem w obszarze służby geodezyjnej i kartograficznej. Odnalezienie produktów z poziomu serwisu możliwe jest dzięki zastosowaniu kryteriów opisowych i przestrzennych, zaprezentowaniu predefiniowanych pakietów danych zaś obsługa produktów dotyczy materiałów w formie cyfrowej oraz analogowej. Prócz tradycyjnej drogi dostarczenia produktów planowane jest też udostępnienie usług transformacji i pobierania danych umożliwiających przekazanie zakupionych danych klientowi – w myśl jednego z zapisów rozporządzenia Ministra Administracji i Cyfryzacji z dn. 5 września 2013 r. w sprawie organizacji i trybu prowadzenia państwowego zasobu geodezyjnego i kartograficznego.

Geoportal/Broker INSPIRE

Broker INSPIRE jest centralnym punktem dostępowym do krajowych danych, określonych w Dyrektywie INSPIRE, z wykorzystaniem rozwiązań technicznych zgodnych z wymaganiami zawartymi w Dyrektywie oraz jej przepisach implementacyjnych. Zgodnie z wymaganiami interoperacyjności oraz przepisami implementacyjnymi, broker udostępnia dane w takiej samej strukturze, z wykorzystaniem tych samych usług oraz w formie wizualnej identycznej jak pozostałe państwa członkowskie UE. Poprzez serwer katalogowy brokera INSPIRE, metadane opisujące wszystkie polskie zbiory danych i usług INSPIRE zostaną udostępnione publicznie. Analogicznie usługi danych przestrzennych – spełniając założenia interoperacyjności i przepisów implementacyjnych w ramach INSPIRE będą udostępnione poprzez broker. Należy również zaznaczyć, że broker dostarcza narzędzia do obsługi sprawozdawczości wymaganej przez Komisję Europejską dot. procesu wdrażania Dyrektywy INSPIRE w Polsce.

Tematy warstw dostępne w ramach modułu:

- INSPIRE: Adresy;
- INSPIRE: Nazwy geograficzne;
- INSPIRE: Działki katastralne;
- INSPIRE: Jednostki administracyjne;
- INSPIRE: Transport BDO;
- INSPIRE: Transport TBD;

Moduł statystyk

Moduł jest składową centralnego punktu dostępowego. Zawiera on opracowania w postaci kartogramów i kartodiagramów przedstawiające w formie wizualnej dane statystyczne w odniesieniu wojewódzkim i powiatowym. Dodatkowo moduł umożliwia opracowywanie kartogramów (według

unikalnych wartości oraz według przedziałów wartości) i kartodiagramów (prostych, kołowych, słupkowych) na podstawie własnych danych z wykorzystaniem specjalnie sformatowanego szablonu pliku *.xls

Aktualnie dostępne warstwy w ramach modułu:

- 7 kartogramów;
- 11 kartodiagramów.

Punkt dostępowy (http://mapy.geoportal.gov.pl/imap/) od strony funkcjonalnej został podzielony na trzy poziomy ukierunkowane pod kątem potrzeb użytkowników w korzystaniu z serwisów tego typu:

- poziom prosty;
- poziom rozszerzony;
- poziom pełny.

Możliwości funkcjonalne i nawigacyjne

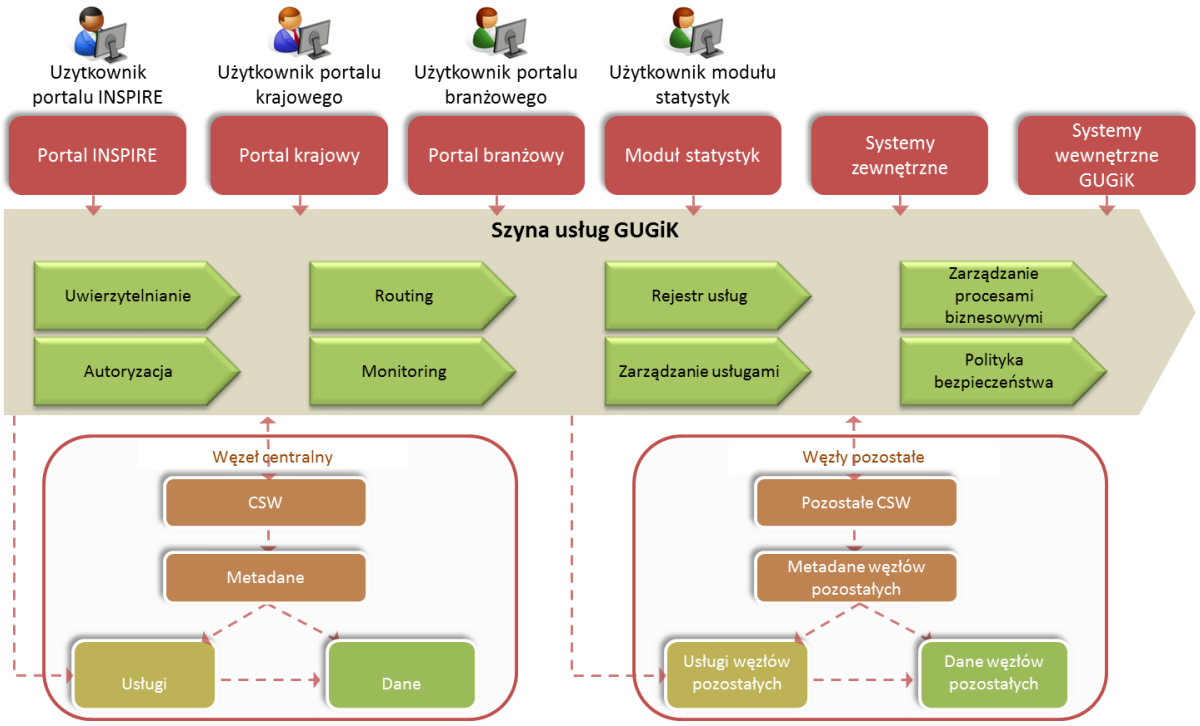
Zakres możliwości funkcjonalnych i nawigacyjnych serwisu wynika z jej domyślnych ustawień. Poziom prosty umożliwia wykonywanie podstawowych operacji stosowanych w geoserwisach (wyszukiwanie obiektów na warstwach, powiększanie przeglądanego obszaru, przełączenie się między geoportalami). Poziom rozszerzony jest wzbogacony o dodatkowe funkcjonalności nawigacyjne. Poziom pełny udostępnia możliwość autoryzowanego dostępu do geoportalu, sporządzanie linków do kompozycji mapowych, tworzenie wraz z zapisywaniem własnych kompozycji mapowych, zgłaszanie błędów, dodawanie usług WMS i WMTS z zewnętrznych serwisów, modyfikację ustawień widoczności warstw i serwisów oraz kontrolek funkcjonalnych, osadzanie kompozycji mapowych, wykonywanie pomiarów odległości i powierzchni, szerszy zakres wyszukiwania (działki, metadane). Geoportal umożliwia personalizowanie funkcjonalności dla poszczególnych poziomów zaawansowania oraz powrót do ustawień domyślnych.

Wersja mobilna

W ramach realizacji projektu Geoportal 2 udostępniono wersję aplikacji przeznaczonej dla urządzeń mobilnych. Aplikacja zapewnia dostęp do rejestrów publicznych zapewnianych przez Główny Urząd Geodezji i Kartografii za pośrednictwem usług centralnego punktu dostępowego. Poszczególne funkcjonalności rozwiązania w dużej mierze odpowiadają funkcjonalnościom aplikacji statycznej (funkcje nawigacyjne, dodawanie usług przeglądania z zewnętrznych serwerów danych

przestrzennych, wyszukiwanie obiektów, proste pomiary), ale pozwalają również śledzić własną pozycję oraz rejestrować, zapisywać, wyświetlać i wysyłać przebytą trasę.

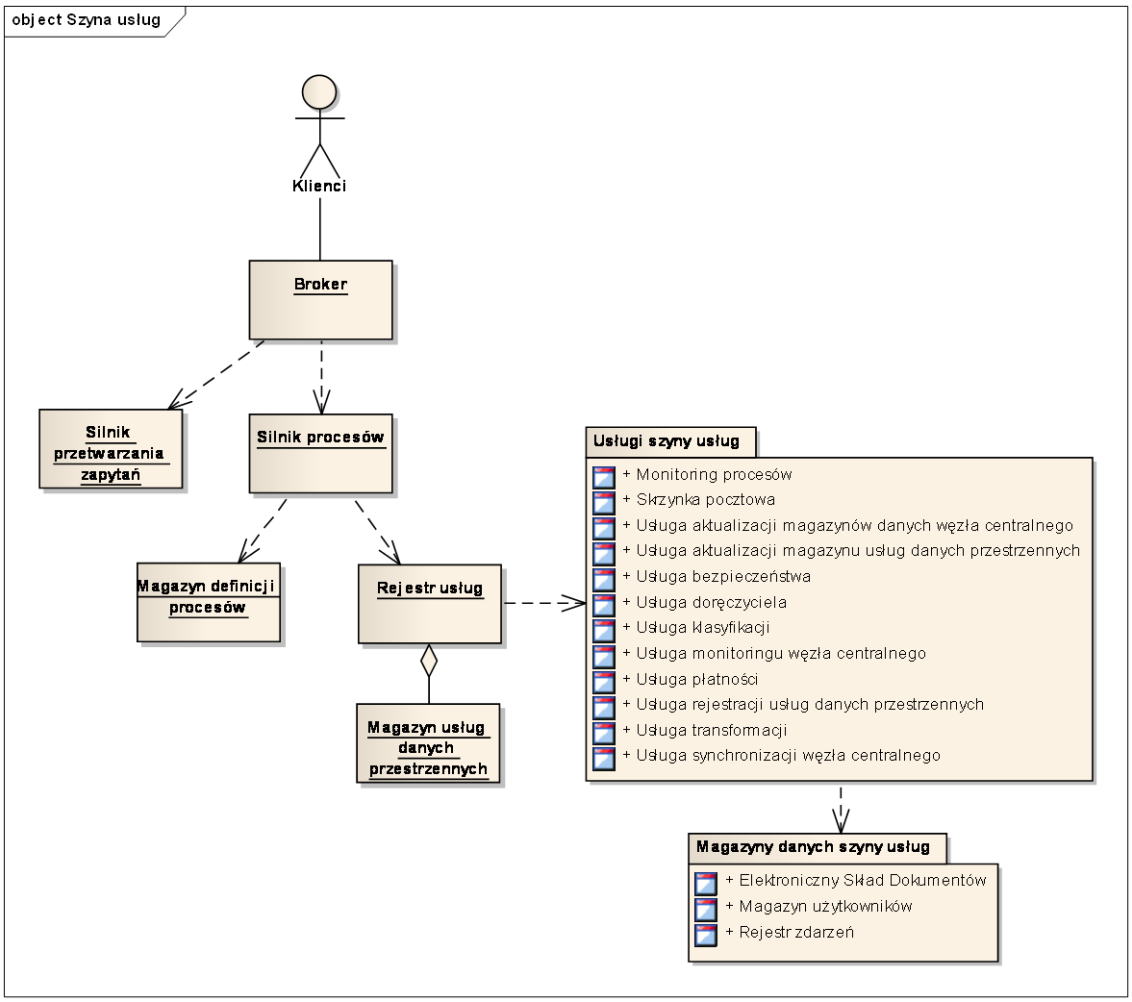
Rysunek 3 Architektura węzła centralnego



Szyna usług systemu Geoportal

Szyna usług systemu Geoportal jest wydzieloną usługą aplikacyjną, która stanowi jednolity punkt dostępu dla wszystkich klientów usług świadczonych przez system Geoportal. Punktem dostępowym dla wszystkich klientów szyny usług jest broker. Broker pełni funkcję brokera krajowego, branżowego, INSPIRE i modułu statystyk. Funkcja portali poszczególnego typu spełniona jest poprzez odpowiednią klasyfikację usług dostępnych w ramach szyny usług. W przypadku żądania klienta do usług określonego rodzaju (np. usług INSPIRE) następuje filtrowanie dostępnych usług zgodnie z zadanym typem.

Rysunek 4 Architektura szyny usług systemu Geoportal



Broker w momencie odebrania żądania klienta posiada informację w jaki sposób przetworzyć zapytania oraz w jaki sposób żądanie uruchomić. Przetwarzaniem zapytań zajmuje się wydzielony komponent, tj. Usługa przetwarzania zapytań. Po przetworzeniu żądanie uruchamia lub odtwarza stan odpowiedniego procesu. Przetwarzaniem procesów zajmuje się silnik przetwarzania procesów. Silnik procesów posiada możliwość uruchomienia procesu na podstawie definicji procesu, odtworzenia stanu procesu w wywołaniu asynchronicznym, monitorowanie stanu i parametrów jakościowych procesu oraz zamknięcie procesu. Definicje procesów są przechowywane w magazynie definicji procesów. Definicje procesów uwzględniają zarejestrowane usługi oraz standardowe operacje związane z definiowaniem procesów (m.in. rozgałęzienia, łączenia, wstrzymania). Szyna usług służy głównie do rejestrowania, ewidencjonowania i wyszukiwania usług. Istnieją dwa typy usług szyny usług systemu Geoportal:

1. Usługi danych przestrzennych,
2. Usługi infrastrukturalne.

Wszystkie usługi są ewidencjonowane w jednolitym rejestrze usług, przy czym umożliwia się hierarchiczne wydzielenie rejestru usług danych przestrzennych oraz rejestru usług infrastrukturalnych. Rejestry zawierają wszystkie dane potrzebne do pokierowania klienta szyny usług do właściwej usługi.

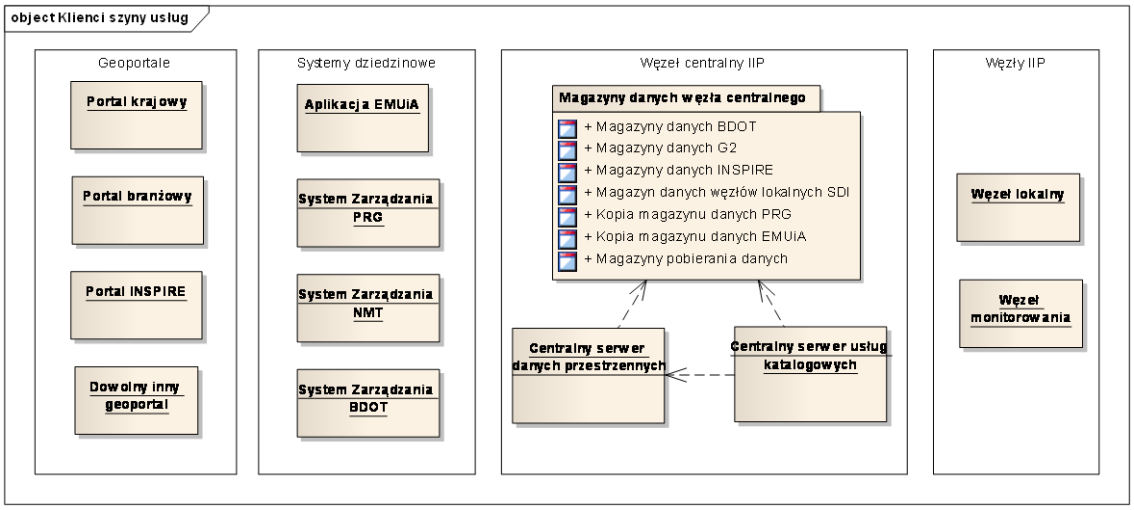
Rejestr usług danych przestrzennych zawiera informacje o wszystkich usługach danych przestrzennych udostępnionych w ramach węzła centralnego IIP oraz ma możliwość rejestracji usług danych przestrzennych wszystkich węzłów IIP.

Szyna usług Geoportal posiada następujące usługi infrastrukturalne:

1. Monitoring procesów
2. Skrzynka podawcza
3. Usługa aktualizacji magazynów węzła centralnego IIP
4. Usługa aktualizacji magazynu usług danych przestrzennych (rejestru)
5. Usługa bezpieczeństwa
6. Usługa doręczyciela (wykorzystująca usługę infrastrukturalną ePUAP)
7. Usługa monitoringu węzła centralnego
8. Usługa płatności
9. Usługa rejestracji usług danych przestrzennych
10. Usługa transformacji
11. Usługa synchronizacji węzła centralnego IIP

wraz z towarzyszącymi magazynami danych (np. Magazyn użytkowników dla usługi bezpieczeństwa, Elektroniczny Skład Dokumentów dla usługi doręczyciela).

Rysunek 5 Klienci szyny usług systemu Geoportal



Podsumowując należy zaznaczyć, że system Geoportal spełnia wyznaczoną mu rolę jako centralnego punktu dostępowego usług wyszukiwania, przeglądania, pobierania, przekształcania i uruchamiania usług danych przestrzennych. Umożliwia łączenie zbiorów danych przestrzennych pochodzących z zasobów różnych organów państwowych w spójną całość, dostępną w formie elektronicznej oraz zapewnia dostęp do danych przestrzennych i usług zgromadzonych zarówno w krajowej jak i w europejskiej infrastrukturze informacji przestrzennej spełniając zapisy art. 13.1 Ustawy o Infrastrukturze Informacji Przestrzennej.

6.2 System PZGiK

System przeznaczony do obsługi centralnej części państwowego zasobu geodezyjnego i kartograficznego składa się z dwóch podstawowych modułów:

- część portalowa umożliwiająca klientom zewnętrznym złożenie wniosku, dokonanie opłaty oraz pobranie danych, zawiera także funkcjonalności dotyczące zarządzania kontami użytkowników i zarządzania kontaktami z klientami

- część wewnętrzna, stanowiąca rozbudowany system kancelaryjny, umożliwiający, poza podstawowymi funkcjonalnościami obsługi spraw i dokumentów, także na integrację z systemami dziedzinowymi, w których gromadzone się dane państwowego zasobu geodezyjnego kartograficznego a także obsługę wymaganych przepisami rejestrów i ewidencji.

6.3 Moduł SDI

Produkt dostarczony w ramach projektu Geoportal 2 określany mianem Modułu SDI, stanowi zestaw oprogramowania dla węzła infrastruktury informacji przestrzennej. Zestaw ten ma na celu zapewnienie przechowywania i udostępniania danych przestrzennych oraz zarządzania zasobami danych o charakterze przestrzennym pozostającymi w gestii podmiotu.

Ponadto rozwiązanie zapewnia możliwość wymiany danych z innymi węzłami infrastruktury informacji przestrzennej. Węzły te należy rozumieć jako podmioty posiadające węzeł SDI w ramach swojej organizacji. Narzędzia zapewniają także synchronizację baz danych przestrzennych przy użyciu usług danych przestrzennych.

Elementy składowe modułu SDI stanowią:

- przestrzenna baza danych

Oprogramowanie jest odpowiedzialne za przechowywanie zbiorów danych przestrzennych oraz pozwala na implementację predefiniowanego schematu bazy danych umożliwiającego działanie węzła w ramach Krajowej Infrastruktury Informacji Przestrzennej. Przestrzenna baza danych umożliwia przechowywanie danych przestrzennych o różnych typach (punkt, linia, powierzchnia, multipunkt, multilinia, multipowierzchnia, kolekcja geometrii) oraz przestrzenne indeksowanie przechowywanych danych wraz z przechowywaniem danych we wskazanym przez użytkownika układzie współrzędnych

- system zarządzania przestrzenną bazą danych

Aplikacja posiada graficzny interfejs użytkownika pozwalający na zarządzanie użytkownikami i ich uprawnieniami, zakładanie i usuwanie baz danych oraz tabel w bazach danych, tworzenie widoków i indeksów, przeglądanie i modyfikowanie danych, a także wykonywanie kopii zapasowych oraz odtwarzanie poprzednich wersji bazy danych.

- narzędzie do zasilania bazy danych SDI

Narzędzie umożliwia zasilanie predefiniowanego schematu bazy danych umożliwiające działanie węzła SDI w ramach Krajowej Infrastruktury Informacji Przestrzennej. Proces zasilania jest konfigurowalny poprzez wybór formatu danych, źródła danych, docelowej bazy oraz układu współrzędnych (m.in.WGS84, 1992, 2000). Czynności związane z przetwarzaniem danych są monitorowane. Szczególnie dotyczy to wersjonowania obiektów zbiorów danych. W przypadku napotkania błędów podczas próby importu narzędzie raportuje błędy i informuje o prawdopodobnej przyczynie niepowodzenia procesu importu.

- serwer danych przestrzennych

Aplikacja odpowiedzialna za możliwość publikacji usług danych przestrzennych z różnych danych źródłowych (m.in. Oracle, PostgreSQL, pliki shp, GML, GeoTIFF), a wszystkie usługi są w pełni konfigurowalne na podstawie autoryzowanego dostępu. Aplikacja umożliwia udostępnianie usług sieciowych z jednego źródła bazodanowego pod różnymi adresami sieciowymi.

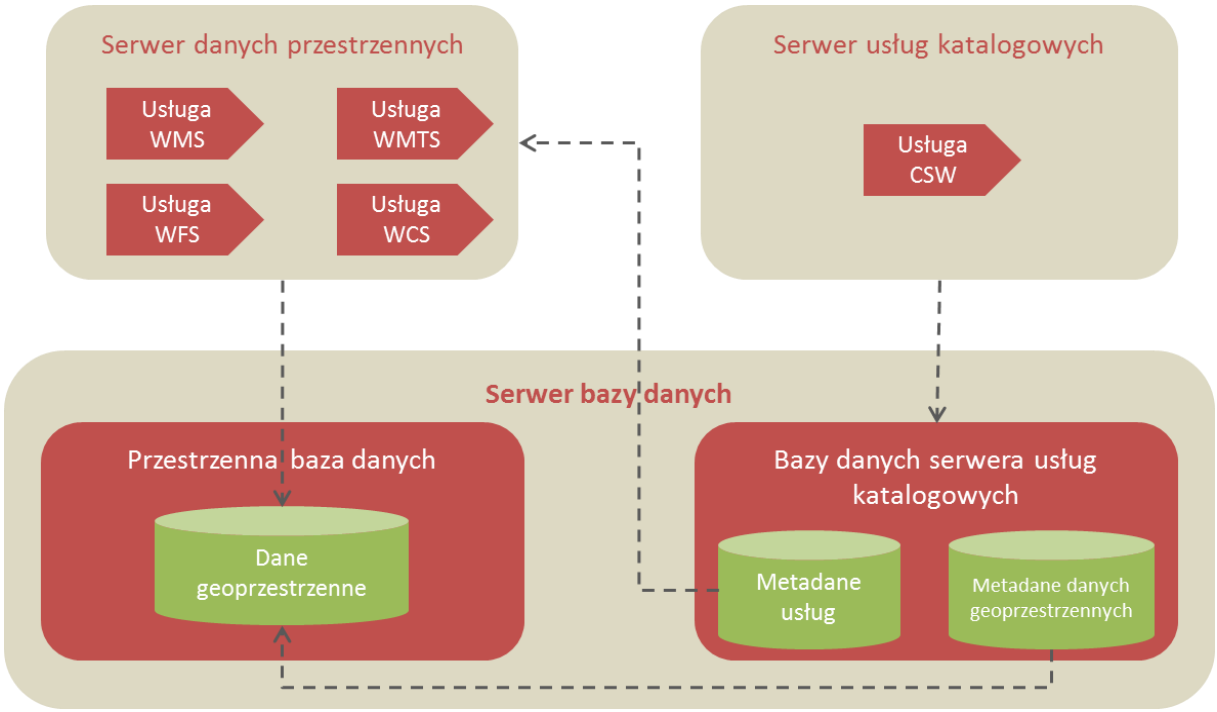
- serwer usług katalogowych

Aplikacja odpowiedzialna za przechowywanie i udostępnianie zasobu metadanych interesariusza. Zapewnia przeszukiwanie zbiorów metadanych, import metadanych z plików XML oraz import metadanych w trybie harvestingu. Aplikacja jest zintegrowana z edytorem i walidatorem metadanych.

- narzędzia do zarządzania synchronizacją węzłów lokalnych

Narzędzia są fizycznie zainstalowane w węźle centralnym IIP. Dzięki temu spełniają rolę zarządczą w przepływie danych w ramach infrastruktury danych przestrzennych. Umożliwiają zasilenie przestrzennej bazy danych węzła centralnego danymi przestrzennymi węzłów lokalnych oraz pozwalają na podział węzłów lokalnych na grupy i przypisanie do poszczególnych grup węzłów określonych modeli synchronizacji. Narzędzia umożliwiają skonfigurowanie parametrów synchronizacji takich jak zakres synchronizowanych danych, kierunek ich przepływu oraz określenie wybranego modelu synchronizacji wraz z raportowaniem procesów synchronizacji.

Rysunek 6 Elementy składowe lokalnego węzła SDI.



Za pomocą wymienionych narzędzi, Moduł SDI posiada mechanizmy zapewniające dowolnemu podmiotowi posiadającemu zbiory danych przestrzennych oraz metadane ich przechowywanie oraz dalsze udostępnianie odbiorcom danych poprzez standardowe usługi danych przestrzennych (wyszukiwania, przeglądania i pobierania). Dzięki temu możliwa jest komunikacja pomiędzy węzłami w ramach krajowej infrastruktury informacji przestrzennej oraz jest zachowana interoperacyjność zbiorów i usług danych przestrzennych.

Niezwykle istotnym walorem wykorzystania modułu jest fakt, iż podmiot będący w jego posiadaniu staje się uczestnikiem Krajowej Infrastruktury Informacji Przestrzennej i dzięki temu ma zapewniony nieodpłatny dostęp do zasobów danych przestrzennych Głównego Urzędu Geodezji i Kartografii oraz może udostępniać i pobierać dane przestrzenne pochodzące od innych interesariuszy korzystających z Modułu SDI (Art. 5 Ustawy Prawo Geodezyjne i Kartograficzne; Art. 17 Ustawy o IIP). Wiodącą rolę w uzgodnieniach dotyczących współdzielenia i współtworzenia zasobów danych przestrzennych pełni Główny Urząd Geodezji i Kartografii (Art. 18, 19 Ustawy o IIP). Założeniem wykorzystania Modułu SDI jest bezpłatne wykorzystanie narzędzi przez zainteresowane podmioty. Pozyskanie Modułu SDI nie wymaga zakupu licencji, jest bezpłatne, a warunkiem sfinalizowania możliwości korzystania z Modułu SDI jest podpisanie porozumienia pomiędzy Głównym Urzędem Geodezji i Kartografii, a zainteresowanym podmiotem.

Warianty hostowania

Zaletą Modułu SDI jest wsparcie czterech modeli hostingu zróżnicowanych w zależności od potrzeb podmiotu wdrażającego. Trzy z nich wykorzystują środowisko wirtualizacyjne potrzebne do uruchomienia maszyn wirtualnych ze zdefiniowanym serwerem danych przestrzennych lub serwerem usług katalogowych oraz przewidują wydzieloną przestrzeń na bazy danych poszczególnych węzłów.

Model 1 – hostowanie wszystkich elementów węzła – wariant ten przewiduje hostowanie wszystkich elementów węzła (metadane, dane oraz usługi serwera katalogowego i serwera danych przestrzennych). Jedynym elementem po stronie interesariusza pozostaje narzędzie do zasilania bazy danych węzła lokalnego służące do zasilania przestrzennej bazy danych danymi należącymi do podmiotu.

Model 2 – hostowanie metadanych i serwera usług katalogowych – w tym wariancie hostowane są elementy związane z metadanymi i usługami serwera katalogowego. Po stronie interesariusza pozostają zaś elementy: przestrzenna baza danych wraz z narzędziami do jej zasilania danymi podmiotu, narzędzia do zarządzania przestrzenną bazą danych oraz serwer danych przestrzennych.

Model 3 – hostowanie danych i serwera danych przestrzennych – wariant ten przewiduje hostowanie wyłącznie danych przestrzennych i serwera danych przestrzennych. Po stronie interesariusza pozostaje baza metadanych wraz z narzędziami zarządzania, serwer usług katalogowych oraz narzędzia do zasilania bazy danych węzła podmiotu.

Wariant ten przeznaczony jest dla jednostek które w ramach własnego węzła lokalnego nie posiadają usług serwera katalogowego. W tej sytuacji wszystkie metadane udostępnione są przy użyciu centralnego serwera katalogowego.

Model 4 – zapewnienie oprogramowania

Wariant ten jest ukierunkowany w stronę podmiotów posiadających pełną infrastrukturę sprzętową umożliwiającą wdrożenie i uruchomienie węzła infrastruktury informacji przestrzennej. W przypadku takich jednostek możliwe jest dostarczenie wyłącznie oprogramowania węzła SDI. Tym samym brak tu jest hostowania elementów węzła sensu stricte przez dostarczyciela. Za czynności te jest odpowiedzialny podmiot, który pobiera oprogramowanie wraz z wszelkimi instrukcjami administratora i użytkownika pozwalające na konfigurację wszystkich elementów we własnym zakresie.

W zależności od decyzji o wyborze konkretnego wariantu hostowania Modułu za utrzymanie i administrowanie poszczególnych jego elementów odpowiedzialny jest CODGiK lub użytkownik Modułu.

Rysunek 7 Warianty hostowania Modułu SDI

		Model 1	Model 2	Model 3	Model 4
Hostowane elementy	Metadane	√	√		
	Serwer usług katalogowych	√	√		
	Dane	√		√	
	Serwer danych przestrzennych	√		√	

6.4 Uniwersalny Moduł Mapowy

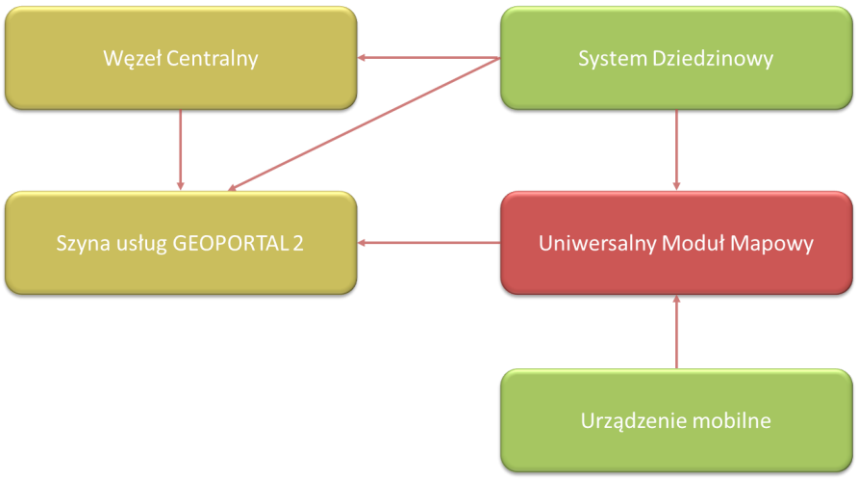
W ramach projektu Geoportal 2 opracowano Uniwersalny Moduł Mapowy. Jest to komponent mapowy możliwy do wykorzystania w systemach wspomagania dowodzenia, wykorzystujący Moduł SDI. Zawiera rozwiązania dedykowane służbom mundurowym i ratowniczym związane z wykorzystaniem referencyjnych oraz operacyjnych danych przestrzennych.

Funkcjonalnie UMM podzielono na rozwiązania dedykowane trzem typom użytkowników wykorzystujących oprogramowanie. Aplikacja dyspozytor umożliwia m.in. wprowadzanie do systemu pozycji obiektów, zdarzeń i incydentów, analizowanie danych oraz wykonywanie prostych pomiarów

– powierzchni i odległości. Aplikacja użytkownik urządzenia mobilnego daje możliwość odczytu bieżącego położenia, wyznaczania tras między wskazanymi punktami w przestrzeni, wyszukiwania obiektów o zadanych kryteriach oraz możliwości analityczne związane z pomiarem odległości. Aplikacja analityk umożliwia integrowanie danych przestrzennych pochodzących z różnych źródeł. Ponadto zawiera funkcjonalności, których efektem jest możliwość opracowania map gęstości i częstości występowania określonych zjawisk niepożądanych na wybranym obszarze, a także generowania szablonów wydruków, raportów i form wizualnych w postaci wykresów, kartogramów i diagramów. Rozwiązanie umożliwia także analizowanie danych Państwowego Zasobu Geodezyjnego i Kartograficznego i zgromadzone w środowisku interesariusza (analizy atrybutowe, przestrzenne oraz na danych rastrowych).

W Uniwersalnym Module Mapowym zaimplementowano ponadto interfejs generyczny umożliwiający wywoływanie wszystkich funkcji w nim zaimplementowanych. Funkcje te nie są powiązane ze specyfiką służb dla których dedykowany był Uniwersalny Moduł Mapowy, a jedynie na podstawie wskazania metody i materiałów wejściowych prezentują wynik wykonywanej operacji. Decyduje to o uniwersalności opracowanego rozwiązania i możliwości jego wykorzystania nie tylko w dowolnych służbach mundurowych ale i innych jednostkach administracji publicznej.

Rysunek 8 Architektura Uniwersalnego Modułu Mapowego

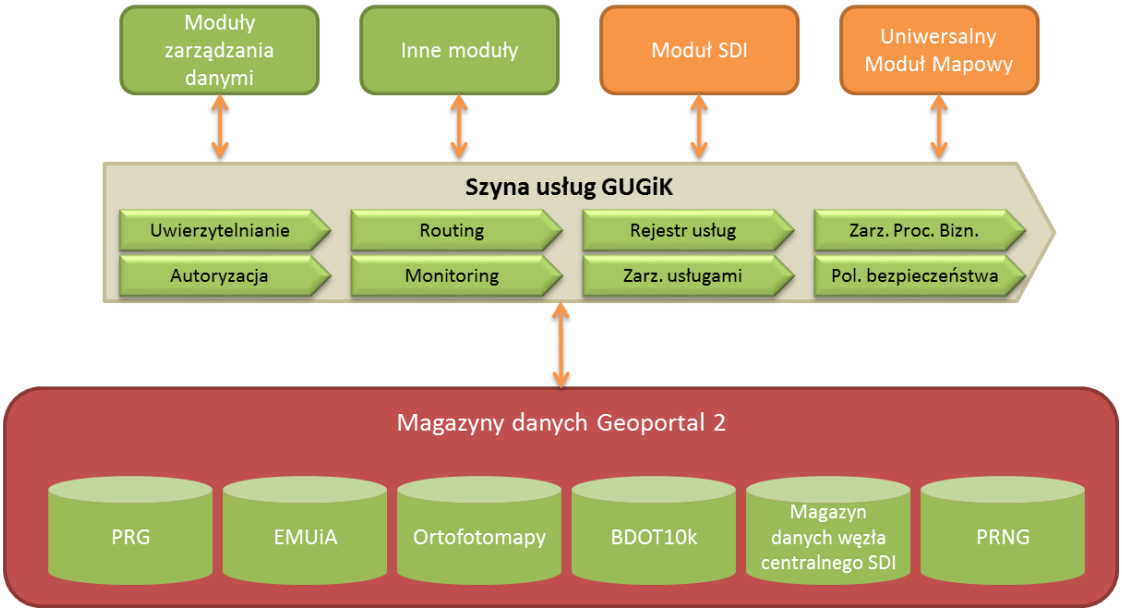


Warte odnotowania jest, iż w dniu 7 listopada 2013 roku Główny Geodeta Kraju podpisał porozumienie z Komendantem Głównym Policji w sprawie wykorzystania Uniwersalnego Modułu Mapowego. Do stycznia 2014 roku Moduł został wdrożony w znacznej części jednostek policji w kraju. Porozumienie przewiduje wykorzystanie danych oraz opisanych wyżej narzędzi sporządzonych w ramach projektu Geoportal 2 w Systemie Wspomagania Dowodzenia Policji. Tym samym systemy policyjne zostaną wzbogacone wizualizacją przestrzenną zgłoszeń oraz zdarzeń rejestrowanych przez służbę. Narzędzia pozwolą m.in. na wskazanie miejsc zdarzeń, określenie dróg

dojazdu oraz umożliwią wizualizację i analizę zgłoszeń wynikającą z ich umiejscowienia w przestrzeni. Taka specyfika wykonywania zadań oraz wykorzystania narzędzi pozwoli na określenie miejsc szczególnie zagrożonych przestępczością, wypadkami drogowymi lub innymi zdarzeniami niepożądanymi.

Ponadto Uniwersalny Moduł Mapowy jest gotowy do wykorzystania przez Systemy Wspomagania Dowodzenia w Państwowej Straży Pożarnej, Państwowym Ratownictwie Medycznym, Wojewódzkich Centrach Powiadamiania Ratunkowego oraz w Agencji Bezpieczeństwa Wewnętrznego.

Rysunek 9 Moduł SDI i Uniwersalny Moduł Mapowy na tle architektury systemu Geoportal.



6.5 Narzędzia do zarządzania metadanymi

W ramach Projektu Geoportal 2 dostarczono aplikacje służące przygotowaniu, walidacji oraz generowaniu metadanych:

Edytor metadanych - Narzędzie umożliwiające zarządzanie metadanymi, w tym przygotowanie nowych plików metadanych oraz edycję istniejących. Jest aplikacją dostępną z poziomu przeglądarki internetowej przy użyciu autoryzowanego dostępu. Dostęp jest ustanawiany przez uprawnionego pracownika Centralnego Ośrodka Dokumentacji Geodezyjnej i Kartograficznej po uprzednim wysłaniu korespondencji elektronicznej z prośbą o wygenerowanie loginu i hasła dla wnioskującego. Aplikacja jest też dostępna bez danych uwierzytelniających, jednak jest to równoznaczne z okrojeniem jej funkcjonalności. Funkcjonalności dostępne bez autoryzacji to:

- tworzenie pliku metadanych;
- załadowanie lokalnego pliku metadanych;

- podgląd pliku metadanych;
- edycja pliku metadanych;
- walidacja pliku metadanych;

Od strony funkcjonalnej narzędzie podzielone zostało na cztery grupy (edycja metadanych, walidacja metadanych, zarządzanie identyfikatorami zasobu oraz zarządzanie aplikacją).

Najobszerniejsza funkcjonalność związana jest z tworzeniem nowych i edytowaniem istniejących plików metadanych. Utworzenie nowego pliku poprzedzone jest wyborem typu zbioru, dla którego chce się opracować metadane (zbiór, seria, usługa) oraz profilu dla którego ma zostać utworzony plik metadanych (ISO, INSPIRE, PZGiK, EGiB, EMUiA, NMT, ORTO, ZOBRAZOWANIA).

W ramach dwunastu zakładek (metadane na temat metadanych, identyfikacja zasobu, położenie geograficzne, odniesienie czasowe, organizacja odpowiedzialna, informacje o zarządzaniu zasobem, słowa kluczowe, warunki dostępu i użytkowania danych, jakość i ważność, klasyfikacja danych przestrzennych, informacje o dystrybucji, zgodność) odpowiadających pakietom metadanych normy ISO 19115 narzędzie pozwala w przyjazny i przejrzysty sposób opisywać zbiory danych przestrzennych. Integracja aplikacji z walidatorem metadanych pozwala na weryfikację sporządzanego pliku w trakcie edycji bądź po jego opracowaniu.

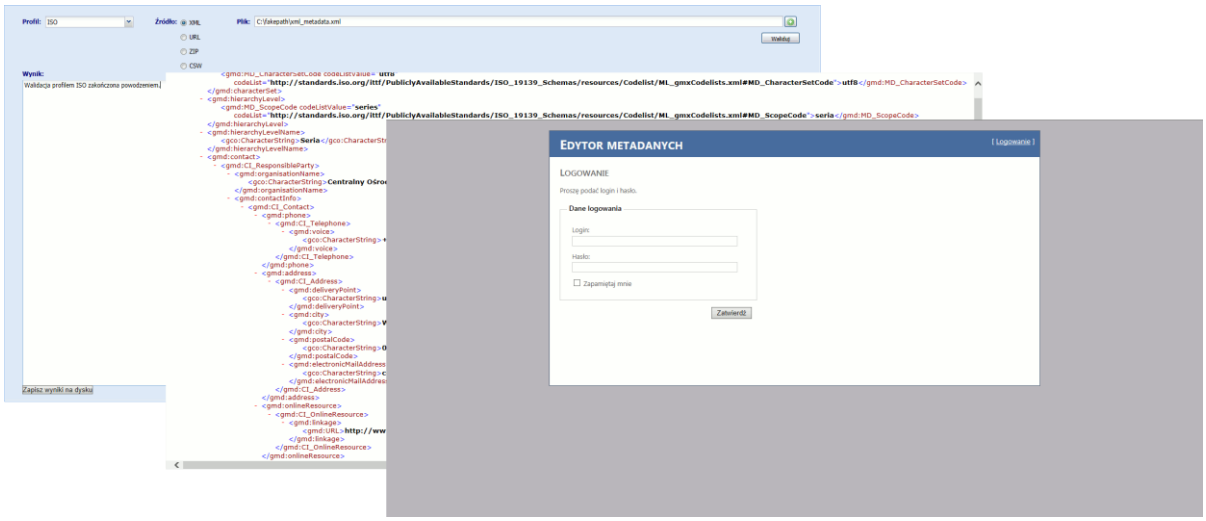
Aplikacja posiada również funkcjonalność publikacji plików metadanych, wcześniej poprawnie zwalidowanych oraz elementy związane z tworzeniem, zarządzaniem i pracą przy wykorzystaniu szablonów metadanych (jest zintegrowana z generatorem metadanych).

Walidator metadanych – aplikacja służąca walidacji metadanych, dostępna – identycznie jak edytor – on-line, jednak nie wymagającą autoryzowanego dostępu. Umożliwia sprawdzenie poprawności pliku metadanych ze schematem aplikacyjnym wybranego profilu metadanych (dostępne profile: ISO, EMUiA, INSPIRE, NMT, ORTO, PZGiK, ZOBRAZOWANIA). Źródło wprowadzanego pliku do walidacji może być zdefiniowane w postaci plików: xml, jako adres URL, skompresowany plik ZIP lub usługa CSW. Walidator umożliwia także raportowanie z przeprowadzonego procesu walidacji poprzez wykazanie ewentualnych błędów w walidacji oraz informuje o wynikach walidacji (powodzenie, niepowodzenie).

Aplikacja poza wymienionymi sposobami walidacji metadanych z poziomu aplikacji przeglądarkowej została również opracowana w formie usługi sieciowej WPS dostępnej pod adresem: http://walidator.geoportal.gov.pl/WPSValidator/WPSValidatorService.svc/get?service=WPS&request=GetCapabilities

Generator metadanych – aplikacja służąca automatycznemu, hurtowemu tworzeniu metadanych dla zasobów danych przestrzennych. W procesie tym wykorzystywane jest powielanie predefiniowanych szablonów i ich jednoczesne uzupełnianie informacjami dotyczącymi metadanych. Narzędzie umożliwia też aktualizację istniejących plików metadanych oraz wspiera generowanie wielojęzycznych plików metadanych. Aplikacja jest zintegrowana z walidatorem metadanych. Realizowane jest to przez bezpośrednie wykorzystanie komponentu walidującego z aplikacji walidator metadanych, a nie podłączenie do usługi sieciowej walidatora.

Rysunek 10 Metadane walidator, edytor.



Dostarczone i udostępnione narzędzia do zarządzania metadanymi umożliwiają podmiotom zewnętrznym zarządzanie metadanymi zgodnie z aktami prawnymi oraz normami i standardami, a także zapewniają możliwość opracowania i udostępniania metadanych zgodnie z wymogami Dyrektywy INSPIRE.

6.6 Narzędzia do harmonizacji zbiorów danych przestrzennych

W ramach realizacji Projektu Geoportal 2 dostarczone zostały narzędzia, które umożliwiają wykonanie harmonizacji zbiorów danych zgodnie z wytycznymi ze Strategii harmonizacji. Narzędzia obecnie są dostosowane do wykonywania harmonizacji dla wybranych zbiorów danych dla tematów z Załączników I, II i III Dyrektywy INSPIRE.

6.7 System Zarządzania Numerycznym Modelem Terenu

System Zarządzania Numerycznym Modelem Terenu (SZNMT) wytworzony został w ramach Projektu ISOK. Podstawowym zadaniem Systemu jest zarządzanie danymi fotogrametrycznymi. Wszystkie dane prowadzone w SZNMT są częścią państwowego zasobu geodezyjnego i kartograficznego

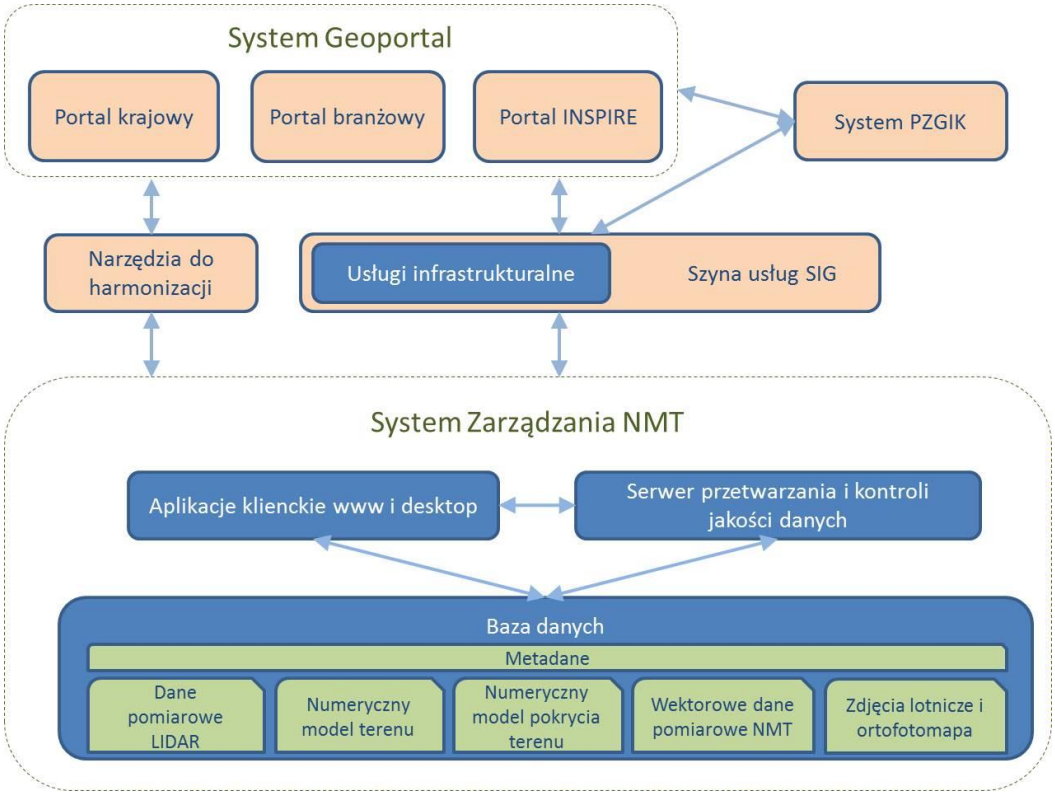
(PZGiK). Zarządzanie danymi fotogrametrycznymi w SZNMT polega na wsparciu zadań GGK i CODGIK związanych z obsługą danych w pzgik, do których należą:

- obsługa zgłoszeń prac geodezyjnych na dostarczenie produktów fotogrametrycznych w zakresie zleceń Głównego Geodety Kraju oraz zgłoszeń prac geodezyjnych dla prac zgłaszanych w CODGiK,
- kontrola jakości danych fotogrametrycznych przed włączeniem danych do PZGiK oraz obsługa zgłoszeń błędów pochodzących od zewnętrznych użytkowników danych fotogrametrycznych,
- włączanie i wyłączanie danych fotogrametrycznych do/z państwowego zasobu geodezyjnego i kartograficznego,
- udostępnianie danych odbiorcom bezpośrednio z SZNMT, za pośrednictwem usług sieciowych danych przestrzennych dostępnych w serwisie www.geoportal.gov.pl oraz poprzez System PZGIK.

System podzielony został na obszary funkcjonalne, w ramach których opracowane zostały funkcje realizujące wyżej wymienione zadania. Oprócz obszarów głównych, do których należą Obsługa zgłoszeń prac, Zarządzanie jakością, Aktualizacja bazy danych, Udostępnianie danych, wyróżnione zostały jeszcze obszary pomocnicze, wspierające główne procesy: Administrowanie systemem, Zarządzanie danymi, Zarządzanie metadanymi, Raportowanie.

SZNMT jest systemem wewnętrznym komunikującym się z pozostałymi systemami SIG poprzez szynę usług Geoportal. Fizycznie SZNMT składa się z komponentów: aplikacja www, aplikacja desktop, serwer przetwarzania i kontroli danych, baza danych. Architektura SZNMT i jego otoczenie przedstawiono na Rysunek 11 Architektura i otoczenie Systemu Zarządzania NMT. Aplikacja www jest podstawową aplikacją kliencką zapewniającą obsługę wszystkich procesów od strony formalnej. Integracja z Systemem PZGIK ma na celu umożliwienie obsługi zgłoszeń prac geodezyjnych i kartograficznych oraz wszelkich wniosków z zakresu obsługi danych fotogrametrycznych poza systemem PZGiK. Aplikacja desktop to narzędzie zbudowane w oparciu o oprogramowanie GIS, mające na celu obsługę manualnych procesów kontroli danych, zarządzania danymi, analiz i wizualizacji.

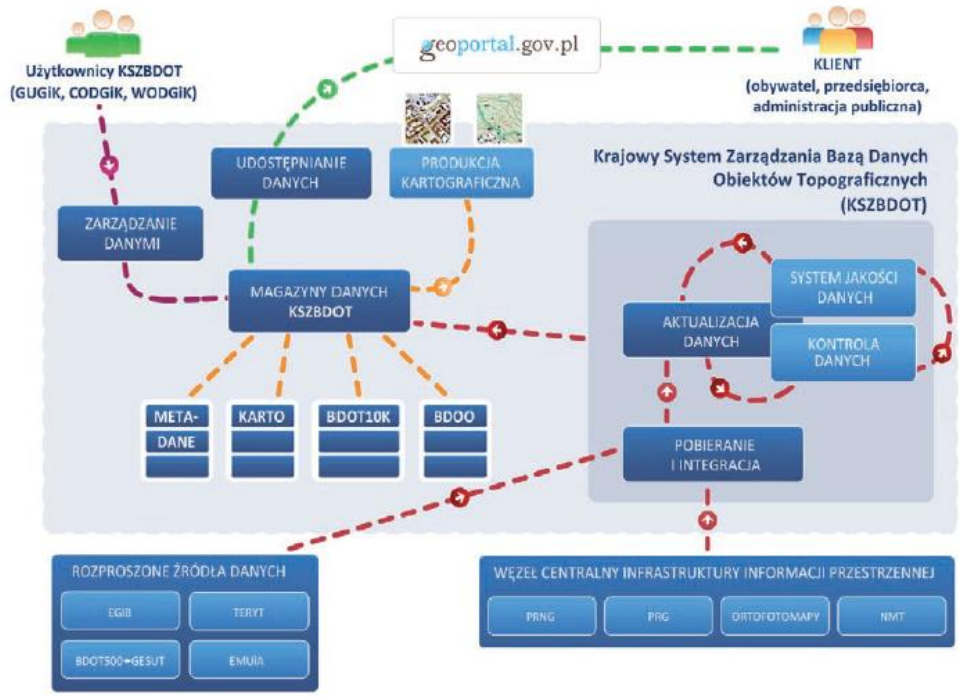
Rysunek 11 Architektura i otoczenie Systemu Zarządzania NMT



6.8 Krajowy System Zarządzania Bazą Danych Obiektów Topograficznych

Krajowy System Zarządzania Bazą Danych Obiektów Topograficznych (KSZBDOT) zbudowany został w ramach Projektu GBDOT. KSZBDOT to system teleinformatyczny, który umożliwia zarządzanie (w tym: tworzenie, prowadzenie i udostępnianie) bazą danych obiektów topograficznych (BDOT10k) i bazą danych obiektów ogólnogeograficznych (BDOO). Użytkownikami systemu są przedstawiciele urzędów marszałkowskich (pracownicy WODGiK), CODGiK i GUGiK.

Rysunek 12 Schemat Krajowego Systemu Zarządzania BDOT



W zależności od posiadanych uprawnień pracownicy GUGiK, CODGiK oraz WODGiK mają dostęp do odpowiednich funkcjonalności systemu oraz danych zgromadzonych w odpowiednich magazynach.

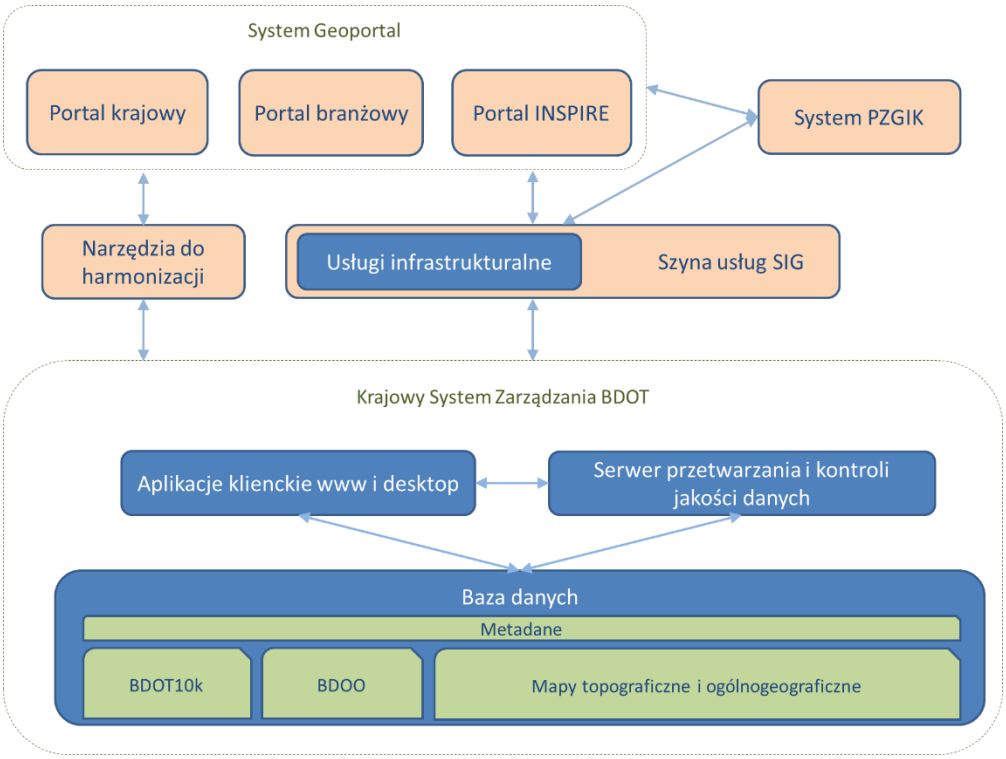
Poszczególne obszary funkcjonalne systemu odpowiadają za:

- aktualizację zbiorów danych BDOT10k oraz BDOO,
- wspieranie procesu tworzenia i aktualizacji standardowych opracowań kartograficznych,
- udostępnianie danych przestrzennych i metadanych na potrzeby publikacji za pomocą usług OGC poprzez portal www.geoportal.gov.pl,
- sprawną i zgodną ze standardami technicznymi kontrolę danych przyjmowanych do państwowego zasobu geodezyjnego i kartograficznego,
- ocenę jakości zbiorów danych,
- realizację generalizacji bazy BDOT10k do bazy BDOO z wykorzystaniem oprogramowania typu ETL.

W Systemie wyodrębnione zostały obszary funkcjonalne - pomocnicze, wspierające główne procesy takie jak: Administrowanie systemem, Zarządzanie danymi, Zarządzanie metadanymi, Raportowanie.

System działa w trybie online, jest dostępny z poziomu przeglądarki internetowej.

Rysunek 13 Architektura i otoczenie Krajowego Systemu Zarządzania BDOT



KSZBDOT jest systemem komunikującym się z pozostałymi systemami SIG poprzez szynę usług Geoportal. Aplikacja www jest podstawową aplikacją kliencką zapewniającą obsługę wszystkich procesów od strony formalnej. Zadania są automatyczne kolejkowane i przetwarzane przez serwery przetwarzania, które są integralną częścią infrastruktury informatycznej KSZBDOT. System KSZBDOT jest zbudowany w oparciu o oprogramowanie GIS, które służy do obsługi manualnych procesów kontroli danych BDOT10k, zarządzania danymi, analiz i wizualizacji a także w oparciu o oprogramowanie typu ETL, które jest wykorzystywane do przeprowadzenia procesu generalizacji.

System podzielny jest na:

- panele użytkowników, które zapewniają dostęp do funkcjonalności systemu przez usługi aplikacyjne,
- magazyny danych, w skład których wchodzą Magazyny danych BDOT10k, BDOO, standardowych opracowań kartograficznych i inne magazyny pomocnicze,
- interfejsy pobierania danych.

Każdy z użytkowników za pośrednictwem paneli KSZBDOT wykorzystuje usługi aplikacyjne systemu, które umożliwiają mu pracę na zbiorach danych znajdujących się w magazynach KSZBDOT. Elementami KSZBDOT są również interfejsy pobierania danych zapewniające komunikację z innymi systemami zarządzania danymi przestrzennymi takimi jak: SZNMT, PRNG. Ponadto za pomocą

interfejsów udostępniania danych, KSZBDOT udostępnia dane dziedzinowe np. BDOT10k, do magazynów węzła centralnego Systemu Geoportal.

6.9 Aplikacja EMUiA

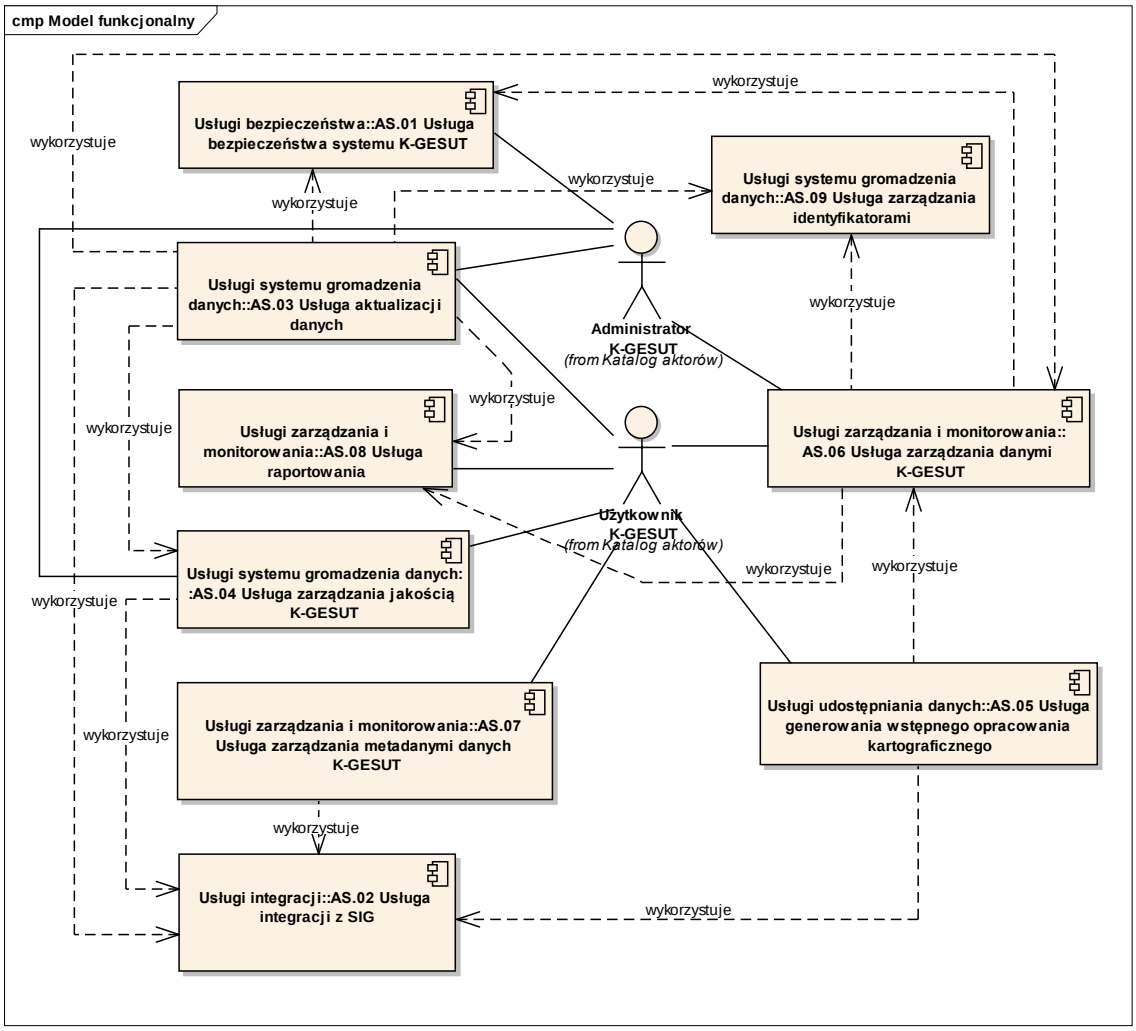
Aplikacja EMUiA została wytworzona w ramach Projektu TERYT 2 i podlegała rozbudowie w ramach Projektu TERYT 3. Aplikacja dostępna jest z poziomu przeglądarki internetowej. Aplikacja przeznaczona jest dla gmin i umożliwia im prowadzenie ewidencji miejscowości, ulic i adresów zgodnie z obowiązującymi przepisami. Aplikacja umożliwia prowadzenie ewidencji, aktualizację danych, a także obsługę wniosków związanych z prowadzeniem ewidencji (np. nadawanie numeru porządkowego).

6.10 System Zarządzania Krajową bazą danych Geodezyjnej Sieci Uzbrojenia Terenu

System Zarządzania Krajową bazą danych Geodezyjnej Sieci Uzbrojenia Terenu (System Zarządzania K-GESUT) to system informatyczny wytworzony w ramach zamówienia na budowę systemu zarządzania K-GESUT. SZ K-GESUT to system teleinformatyczny, który służy do tworzenia, prowadzenia i udostępniania baz danych K-GESUT. Bazy danych K-GESUT zasilane są danymi z baz GESUT prowadzonych przez starostów powiatowych.

Poniższy diagram przedstawia model funkcjonalny systemu K-GESUT. Na diagramie umieszczono usługi aplikacyjne K-GESUT, aktorów korzystających z usług oraz uwidoczniono wzajemne zależności usług aplikacyjnych.

Rysunek 14 Model funkcjonalny systemu zarządzania K-GESUT



Poniżej przedstawiony został szczegółowy opis usług systemu K-GESUT.

Usługi bezpieczeństwa

W ramach usług bezpieczeństwa wyróżniono jedną usługę aplikacyjną.

AS.01Usługa bezpieczeństwa systemu K-GESUT

- Kontrola bezpieczeństwa systemu K-GESUT;
- Zarządzanie aspektami bezpieczeństwa systemu K-GESUT;
- Monitoring prowadzonych w ramach systemu operacji.

Usługi integracji

W ramach usług integracji wyróżniono jedną usługę aplikacyjną.

AS.02 Usługa integracji z SIG

Usługa związana z zarządzaniem udostępniania danych

Usługa systemu gromadzenia danych

W ramach usług systemu gromadzenia danych wyróżniono:

- Usługę aktualizacji danych;
- Usługę zarządzania jakością;
- Usługę zarządzania identyfikatorami.

AS.03 Usługa aktualizacji danych

Usługa realizująca proces aktualizacji krajowej bazy GESUT. Pojęcie "aktualizacja" jest rozumiane jako proces składający się ze wszystkich czynności wykonywanych przez system, od pobrania danych powiatowej bazy GESUT do zasilenia.

Usługa realizuje następujące podprocesy:

- Pobieranie danych powiatowej bazy GESUT oraz metadanych zbiorów danych GESUT usługami danych przestrzennych;
- Pobieranie danych powiatowej bazy GESUT oraz metadanych zbiorów danych GESUT z serwera FTP;
- Weryfikacja danych powiatowej bazy GESUT oraz walidacja metadanych zbiorów danych GESUT;
- Generalizacja obiektów powiatowej bazy GESUT do postaci obiektów krajowej bazy GESUT;
- Aktualizacja danych w magazynie danych produkcyjnych systemu K-GESUT.

AS.04 Usługa zarządzania jakością K-GESUT

Usługa realizująca zadania z zakresu zarządzania jakością danych w systemie K-GESUT.

AS.09 Usługa zarządzania identyfikatorami

Usługa realizująca zadania z zakresu zarządzania identyfikatorami IIP obiektów krajowej bazy GESUT.

Usługi udostępniania danych

W ramach usług udostępniania danych wyróżniono jedną usługę aplikacyjną

AS.05 Usługa generowania wstępnego opracowania kartograficznego

Usługa realizująca zadania z zakresu generowania wstępnego opracowania kartograficznego.

Usługa zarządzania i monitorowania

W ramach usług zarządzania i monitorowania wyróżniono:

- Usługę zarządzania danymi w systemie K-GESUT;

- Usługę zarządzania metadanymi danych w systemie K-GESUT;
- Usługę raportowania.

AS.06 Usługa zarządzania danymi K-GESUT

Usługa realizująca zadania z zakresu zarządzania danymi w systemie K-GESUT.

AS.07 Usługa zarządzania metadanymi danych krajowej bazy GESUT

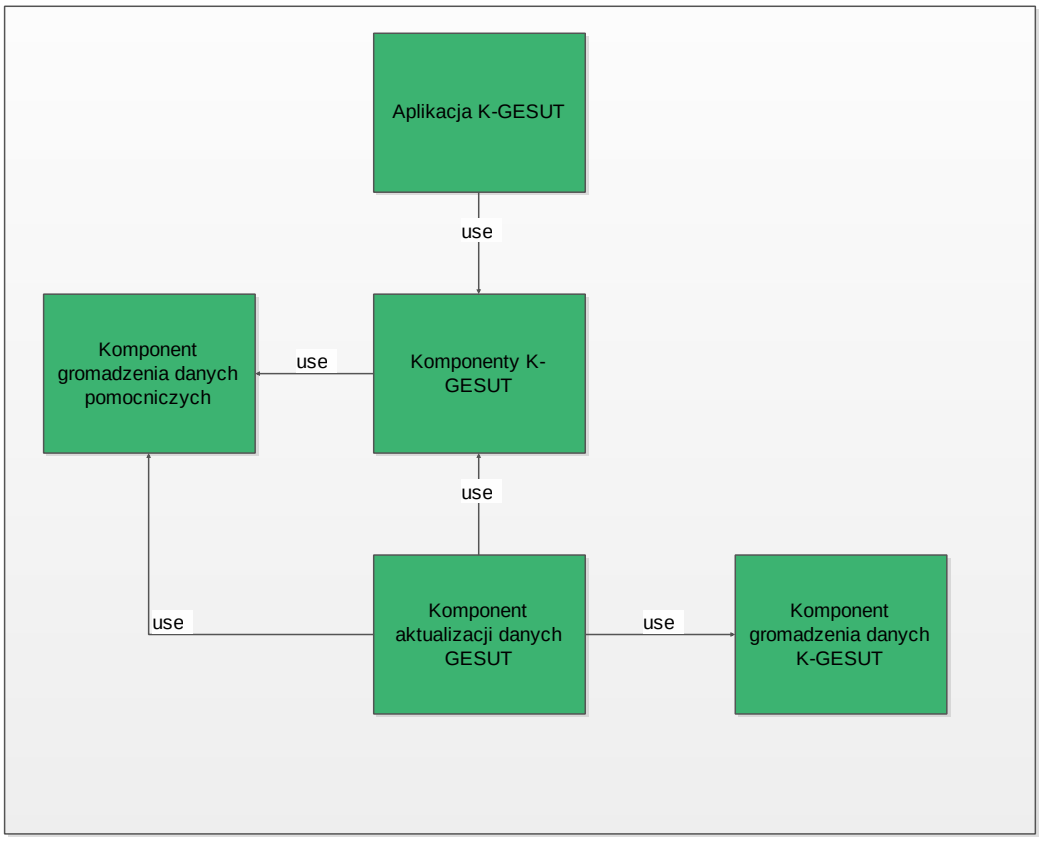
Usługa realizująca zadania z zakresu zarządzania metadanymi danych w systemie K-GESUT

AS.08 Usługa raportowania

Usługa realizująca zadania z zakresu raportowania.

Na poniższym rysunku przedstawiono logiczne elementy systemu oraz powiązania pomiędzy nimi.

Rysunek 15 Architektura logiczna systemu K-GESUT.



Poniżej opisano elementy przedstawione na powyższym rysunku

Aplikacja systemu K-GESUT

Komponent stanowiący interfejs użytkownika systemu, umożliwiający:

- Przeglądanie danych;
- Uruchamianie procesów;
- Przeglądanie wyników procesów.

Realizowane usługi aplikacyjne:

- AS.01 Usługa bezpieczeństwa systemu K-GESUT;
- AS.05 Usługa generowania wstępnego opracowania kartograficznego;
- AS.06 Usługa zarządzania danymi K-GESUT;
- AS.07 Usługa zarządzania metadanymi danych K-GESUT;
- AS.08 Usługa raportowania;
- AS.02 Usługa integracji z SIG.

Komponenty systemu K-GESUT

Komponenty służące do wykonywania operacji na danych w systemie K-GESUT, w tym:

- Walidacja;
- Generalizacja;
- Kontrola jakości.

Realizowane usługi aplikacyjne:

- AS.02 Usługa integracji z SIG;
- AS.03 Usługa aktualizacji danych;
- AS.09 Usługa zarządzania identyfikatorami.

Komponent aktualizacji danych krajowej bazy GESUT

Komponent pozwalający na pobranie aktualizacji danych krajowej bazy GESUT, w tym:

- Pobieranie danych powiatowej bazy GESUT i zasilanie nimi krajowej bazy GESUT;
- Generowanie i walidacja plików metadanych;
- Generowanie raportów błędów danych z powiatowej bazy GESUT i umieszczanie ich na FTP.

Realizowane usługi aplikacyjne:

- AS.03 Usługa aktualizacji danych.

Komponent gromadzenia danych krajowej bazy GESUT

Komponent pozwalający na przechowywanie danych krajowej bazy GESUT.

Komponent gromadzenia danych pomocniczych

Komponent pozwalający na gromadzenie danych pomocniczych.

6.11 System Zarządzania Państwowym Rejestrem Granic i Powierzchni Jednostek Podziałów Terytorialnych Kraju

System Zarządzania Państwowym Rejestrem Granic i Powierzchni Jednostek Podziałów Terytorialnych Kraju (SZPRG) został wytworzony w ramach Projektu TERYT 2 i podlegał rozbudowie w ramach Projektu TERYT 3. System umożliwia prowadzenie rejestru granic jednostek podziału terytorialnego w zakresie zgodnym z rozporządzeniem oraz prowadzenie ewidencji adresów wraz ich lokalizacją przestrzenną. SZPRG zasilany jest m.in. danymi z ewidencji miejscowości, ulic i adresów, prowadzonymi przez gminy.

6.12 Zintegrowany System Informacji o Nieruchomościach

System ZSIN spełnia wymagania nakładane na Główny Urząd Geodezji i Kartografii rozporządzeniem Rady Ministrów z dnia 17 stycznia 2013 r. w sprawie zintegrowanego systemu informacji o nieruchomościach (Dz. U. z 2013 r., poz. 249) oraz wspiera GUGIK w realizacji zadań w zakresie EGiB nakładanych przez ustawę PGiK. W ramach prac ZSIN - Faza I wytworzono Centralne Repozytorium, którego celem jest przechowywanie zintegrowanych danych EGiB z całego kraju.

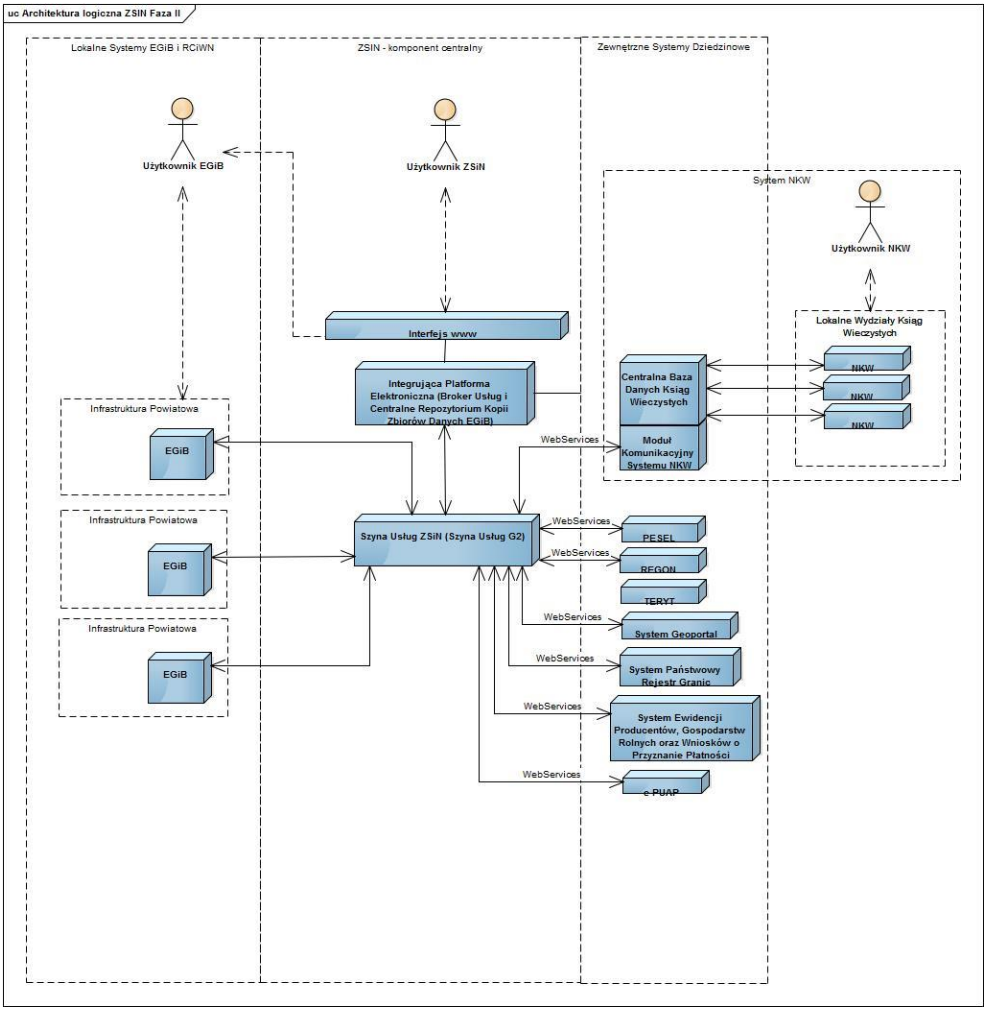
W ramach Projektu ZSIN - Faza I przygotowano integrację z następującymi rejestrami publicznymi:

- EGiB prowadzone przez starostwa powiatowe;
- KSEP prowadzony przez Agencję Rozwoju i Modernizacji Rolnictwa;
- Księgi Wieczyste (system NKW/EKW) prowadzony przez Ministerstwo Sprawiedliwości;
- REGON prowadzony przez Główny Urząd Statystyczny;
- TERYT prowadzony przez Główny Urząd Statystyczny;
- PESEL prowadzony przez Ministerstwo Cyfryzacji (dawniej Ministerstwo Spraw Wewnętrznych) w ramach Systemu Rejestrów Państwowych (SRP);
- PRG prowadzony przez Główny Urząd Geodezji i Kartografii;
- EPN prowadzony przez gminne organy podatkowe.

Podstawową funkcją ZSIN jest wzajemna integracja danych zgromadzonych w bazach danych włączonych do systemu, umożliwienie wymiany i weryfikacji danych pomiędzy tymi bazami oraz prowadzenie centralnego punktu dostępowego do wszystkich danych związanych z nieruchomościami. Funkcjonowanie systemu polega na gromadzeniu i integracji danych EGiB prowadzonych w 380 starostwach, udostępnianiu tych danych w sposób centralny pozostałym

systemom pracującym w ramach ZSIN oraz przesyłanie zawiadomień o zmianach w poszczególnych bazach danych pomiędzy systemami.

Rysunek 16 Model logiczny ZSIN po realizacji Fazy I

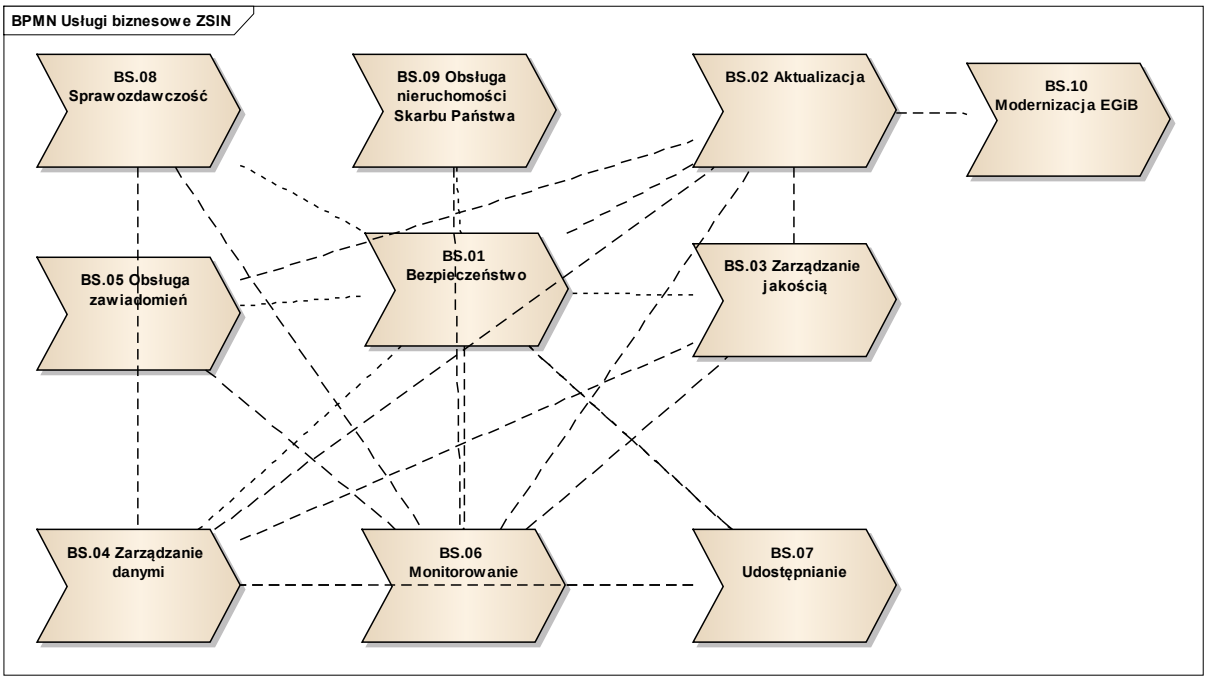


W ramach realizacji Projektu ZSIN - Faza I zaimplementowano następujące **usługi biznesowe**:

- BS.01.Bezpieczeństwo;
- BS.02.Aktualizacja;
- BS.03.Zarządzanie jakością;
- BS.04.Zarządzanie danymi;
- BS.05.Obsługa zawiadomień;
- BS.06.Monitorowanie;
- BS.07.Udostępnianie;
- BS.08.Sprawozdawczość;
- BS.09.Obsługa nieruchomości Skarbu Państwa;
- BS.10.Modernizacja EGiB.

Poniższy diagram przedstawia powiązania pomiędzy poszczególnymi, zaimplementowanymi usługami.

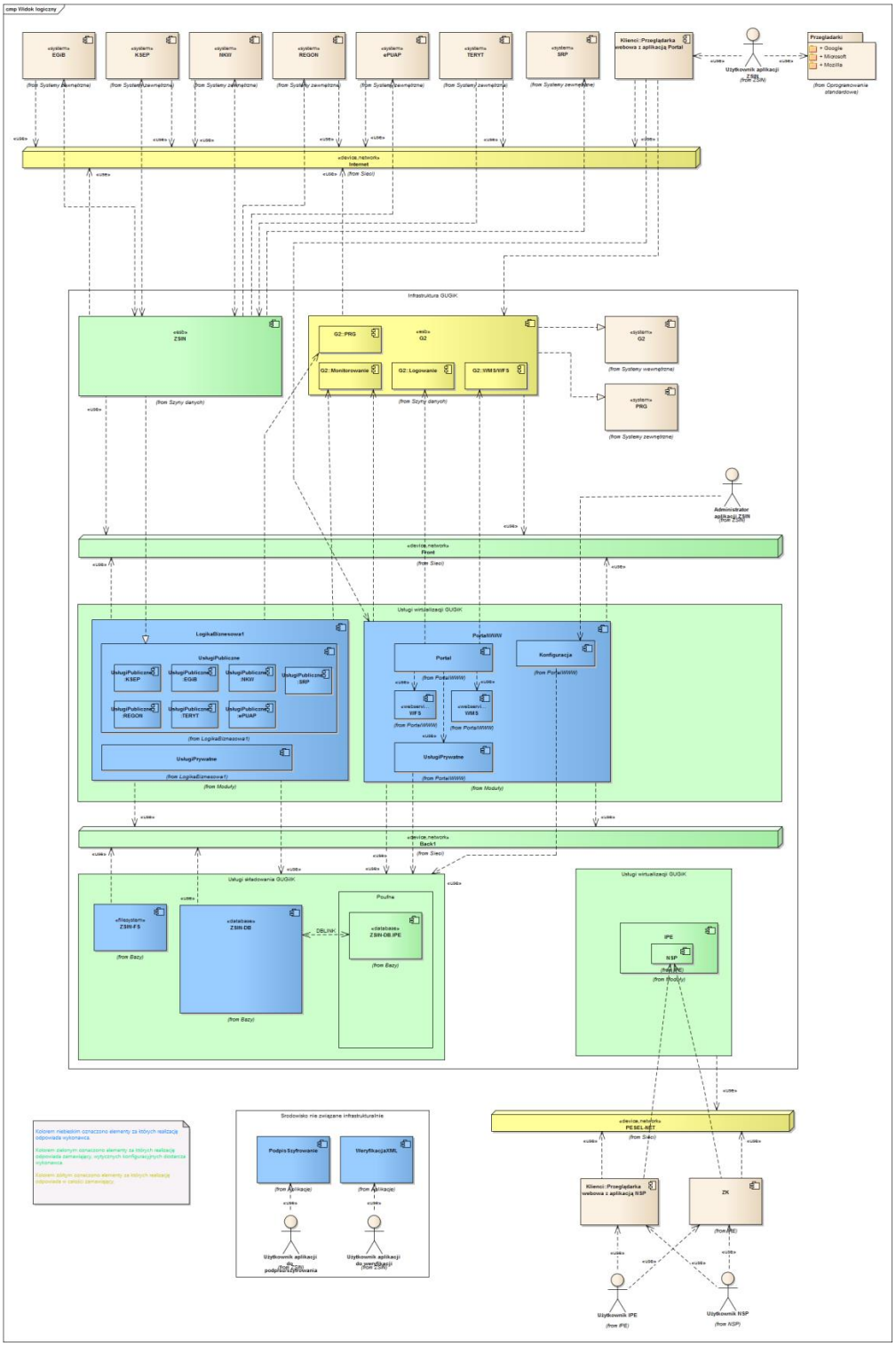
Rysunek 17 Powiązania pomiędzy usługami ZSIN



Oprogramowanie aplikacyjne ZSIN przedstawione jest przy pomocy komponentów technologicznych. Komponenty technologiczne reprezentują wydzielone logicznie przedmioty, których celem jest dostarczenie wymaganych funkcjonalności systemu. Poniżej opisano wszystkie zidentyfikowane komponenty Systemu ZSIN, uwzględniając zależności między nimi, a także z systemami/komponentami zewnętrznymi w stosunku do Systemu ZSIN.

Na poniższym rysunku przedstawiono logiczny model komponentów systemu ZSIN.

Rysunek 18 Logiczny model komponentów systemu ZSIN



Opis elementów modelu:

1. Usługi składowania GUGiK – infrastruktura GUGiK odpowiedzialna ze persystencję danych (środowiska bazodanowe, systemy plików) – składa się na nią oprogramowanie i infrastruktura sprzętowa realizująca przechowywanie i archiwizowanie danych.

2. Usługi wirtualizacji GUGiK – infrastruktura GUGiK odpowiedzialna za wirtualizację sprzętu umożliwiająca zarządzanie sprzętem i hostowanie środowisk komputerowych wraz systemami operacyjnymi i oprogramowaniem aplikacyjnym.
3. Szyna usług ZSIN – szyna usług, która udostępnia publiczne usługi systemu ZSIN (dostępne dla systemów/użytkowników zewnętrznych), a także stanowi punkt dostępowy dla systemu ZSIN do usług zewnętrznych. Szyna usług zapewnia separację systemu ZSIN od sieci publicznych i innych sieci dostępowych (np. sieć Internet).
4. Szyna usług Geoportal – szyna usług w GUGiK udostępniająca usługi systemu Geoportal.
5. Sieć Internet – publicznie dostępna sieć Internet, przez którą możliwy jest publiczny dostęp do systemu ZSIN, jak również komunikacja z systemami zewnętrznymi.
6. Sieć PESEL-NET – sieć systemu PESEL, wykorzystywana obecnie w systemie ZSIN. Ze względu na poufność danych wymienianych w tej sieci wymagana jest „galwaniczna" odizolowanie tej sieci od pozostałych elementów systemu.
7. Sieć „Front" – logiczna infrastruktura sieciowa, za pomocą której realizowany jest dostęp do usług ZSIN, komunikacja z systemami GUGiK, udostępnianie funkcjonalności systemu dla użytkowników w GUGiK.
8. Sieć „Back1" – logiczna infrastruktura sieciowa za pomocą której realizowana jest komunikacja pomiędzy komponentami systemu ZSIN (oprogramowanie aplikacyjne, systemy bazodanowe, systemu plików, etc.).

Na diagramie, w zakresie komunikacji z IPE, jest zamodelowana koncepcja, w której IPE w dalszym ciągu funkcjonuje w sieci PESEL-NET, a baza ZSIN-DB.IPE jest jedynie repliką bazy danych IPE przeniesiona do infrastruktury SIG.

6.13 Systemy planowane do rozwoju i budowy.

Równolegle do niniejszego podstępowania Zamawiający planuje rozwój systemów SIG w ramach działania budowy i udostępniania usług w ramach Projektów CAPAP, ZSIN Faza II i K-GESUT, współfinansowanych ze środków Programu Operacyjnego Polska Cyfrowa Oś 2 Działanie 2.1 „Wysoka dostępność i jakość e-usług publicznych". Zakres prac planowanych do realizacji został opisany w studiach wykonalności dla projektów CAPAP, ZSIN Faza II i K-GESUT, które są załącznikiem do niniejszego dokumentu.

7 Opis techniczny posiadanej infrastruktury

Niniejsza część przedstawia zestawienie infrastruktury.

Dla elementów infrastruktury, dla których wsparcie wygasło, Zamawiający jest w trakcie prowadzenia Postępowań na zakup wsparcia lub planuje uruchomić takie Postępowania.

7.1 Infrastruktura sprzętowa

Poniżej przedstawione komponenty znajdują się w lokalizacji CODGiK.

ID	Nazwa	Ilość	Wsparcie do	Opis
Serwery				
1	IBM BladeCenter HX5	8	31.12.2016	VMware vSphere 6.x
2	IBM BladeCenter HS22V	2	31.12.2016	przeznaczone na szynę usług – OracleVM + Oracle ESB
3	IBM System x3650 M4	1	31.12.2016	backup
4	HP BL660c Gen8	4	10.12.2016	VMware vSphere 6.x
5	HP BL660c Gen8	1	30.12.2019	VMware vSphere 6.x
6	HP BL660c Gen8	2	14.12.2017	VMware vSphere 6.x
7	HP BL660c Gen8	2	09.12.2017	VMware vSphere 6.x
8	HP BL660c Gen8	2	30.09.2018	VMware vSphere 6.x
9	HP BL660c Gen9	2	30.11.2018	VMware vSphere 6.x
10	HP ProLiant	7	brak	monitoring
Klatki Blade				
1	IBM BladeCenter H Chassis	2	31.12.2016	
2	HP BLc7000	1	10.12.2016	
3	HP BLc7000	1	30.12.2019	
Jednolita infrastruktura bazodanowa				
1	Oracle Exadata X2-2 HalfRack z rozbudowaną pamięcią RAM do 1152 GB	1	08.06.2018	1) Rozbudowa pojemności - Exadata Expansion Half Rack HC; 2) Rozbudowa pojemności – 2 serwery Storage X5-2 HC;
Warstwa składowania				
1	IBM SoNAS 2851-RXA	1	31.12.2016	
2	IBM Storwize V7000	1	31.12.2016	
3	IBM Storwize V7000 Gen. 2	1	16.06.2018	
4	IBM TS3310 Tape Library	1	31.12.2016	
5	EMC DataDomain DD2500	1	15.12.2019	stanowi środowisko składowania kopii zapasowych dla maszyn

				wirtualnych oraz baz danych
Warstwa sieciowa				
1	Juniper SRX3400	2	31.12.2017	Firewall Klaster
2	NLB F5 BIG-BT-5250V	2	25.06.2018	klaster active-passive
3	VPN Cisco ASA 5510 K9	1	31.12.2017	
4	Juniper EX2200-24T	4	31.12.2017	
5	Juniper EX4200-48T	4	31.12.2017	
6	Juniper J6350	2	31.05.2015	
7	IBM RackSwitch G8124E	1	31.12.2017	
8	Thales nShield Connect 1500	2	31.12.2017	
9	IBM System Storage SAN B-Type Switch	2	31.12.2017	

7.1.1 Poniżej przedstawione komponenty znajdują się w lokalizacji Katowice.

ID	Nazwa	Ilość	Wsparcie do	Opis
Serwery				
1	IBM System x3650 M4	3	31.12.2016	backup
Warstwa składowania				
1	IBM Storwize V7000	1	31.12.2016	
2	EMC DataDomain DD2500	1	15.12.2019	stanowi replikę danych z EMC DataDomain DD2500 z Warszawy
3	Biblioteka taśmowa IBM TS3310	1	31.12.2016	

7.2 Główna infrastruktura programowa

ID	Nazwa	Wersja	Ilość	Wsparcie do
1.	Oracle Directory Services Plus - Processor Perpetual	12.1.3	2 CPU	31.12.2016
2.	Oracle Directory Services Plus - Named User Plus Perpetual	12.1.3	10 Users	31.12.2016
3.	Oracle SOA Suite for Oracle Middleware - Processor Perpetual	12.1.3	8 CPU	31.12.2016
4.	Oracle SOA Suite for Oracle Middleware - Named User Plus Perpetual	12.1.3	20 Users	31.12.2016
5.	Oracle WebLogic Suite - Processor Perpetual	12.1.3	8 CPU	31.12.2016

6.	Oracle WebLogic Suite - Named User Plus Perpetual	12.1.3	20 Users	31.12.2016
7.	Oracle WebLogic Server Standard Edition - Processor Perpetual	10.3.3.0	12 CPU	31.12.2016
8.	Oracle WebLogic Server Standard Edition - Named User Plus Perpetual	10.3.3.0	40 Users	31.12.2016
9.	Oracle VM	3.3.1	n/d	brak
10.	Oracle Database Enterprise Edition - Processor Perpetual	11.2.0.3.27	28 CPU	31.12.2016
11.	Oracle Database Enterprise Edition - Named User Plus Perpetual	11.2.0.3.27	100 Users	31.12.2016
12.	Oracle Real Application Clusters - Processor Perpetual	11.2.0.3.27	24 CPU	31.12.2016
13.	Oracle Diagnostics Pack - Processor Perpetual	11.2.0.3.27	24 CPU	31.12.2016
14.	Oracle Tuning Pack - Processor Perpetual	11.2.0.3.27	24 CPU	31.12.2016
15.	Oracle Spatial and Graph - Processor Perpetual	11.2.0.3.27	24 CPU	31.12.2016
16.	Oracle Spatial and Graph - Named User Plus Perpetual	11.2.0.3.27	100 Users	31.12.2016
17.	vSphere Enterprise Plus	6.0	72 CPU	brak
18.	vSphere Enterprise Plus	6.0	12 CPU	26.11.2018
19.	vCenter Standard	6.0	1	brak
20.	SYMC NETBACKUP SERVER AND 5 STD CLIENT STARTER PACK 7.6 WIN/LNX/SOLX64 TIER 2 MULTI PROD BNDL	7.6	1	brak
21.	SYMC NETBACKUP ENTERPRISE SERVER 7.6 WIN/LNX/SOLX64 1 SERVER TIER 2	7.6	2	brak
22.	SYMC NETBACKUP CLIENT APPLICATION AND DATABASE PACK 7.6 WIN/LNX/SOLX64 1 SERVER TIER 4	7.6	1	brak
23.	SYMC NETBACKUP CLIENT APPLICATION AND DATABASE PACK 7.6 WIN/LNX/SOLX64 1 SERVER TIER	7.6	1	brak

	1			
24.	SYMC NETBACKUP DATA PROTECTION OPTIMIZATION OPTION 7.6 XPLAT 1 FRONT END TB	7.6	20	brak
25.	SYMC NETBACKUP ENTERPRISE CLIENT 7.6 WIN/LNX/SOLX64 1 SERVER TIER 3	7.6	24	brak
26.	SYMC NETBACKUP ENTERPRISE SERVER 7.6 WIN/LNX/SOLX64 1 SERVER TIER 2	7.6	2	brak
27.	SYMC NETBACKUP OPTION SHARED STORAGE OPTION 7.6 XPLAT 1 DRIVE	7.6	4	brak
28.	SYMC NETBACKUP OPTION LIBRARY BASED TAPE DRIVE 7.6 XPLAT PER DRIVE	7.6	7	brak
29.	SYMC NETBACKUP OPTION NDMP 7.6 XPLAT PER SERVER TIER 4	7.6	1	brak
30.	SYMC NETBACKUP STANDARD CLIENT 7.6 XPLAT 1 SERVER	7.6	2	brak
31.	Trend Micro Deep Security - Anti-malware - per CPU (Socket)	9.6	84 CPU	26.11.2017
32.	MS Windows DataCenter	od 2008 do 2012 R2	42 CPU (84 CPU fizyczne)	brak
33.	HP Service Manager	9.33	1	brak
34.	HP Real User Monitor Engine	9.23	1	brak
35.	HP SiteScope	11.23	751	brak
36.	HP Performance Manager	9.03	1	brak
37.	HP Network Node Manager	9.23	1	brak
38.	HP BSM	9.23	1	brak

7.3 Środowiska przetwarzania

1. Środowisko backup-owe.
2. Środowiska testowe (w szczególności aplikacji, bazy danych, szyny usług).
3. Środowiska produkcyjne (w szczególności aplikacji, bazy danych, szyny usług).
4. Środowisko utrzymania i monitorowania.

7.4 Usługi technologiczne

1. Szyna usług.
2. Usługa warstwy aplikacji.
3. Usługa dostępu do bazy danych.
4. Usługa kopii zapasowych.
5. Usługa utrzymania i monitorowania.
6. Usługa dostępu blokowego SAN.
7. Usługa NAS.

7.5 Zestawienia lokalizacji, w których prowadzone będzie utrzymanie

1. CODGiK, Warszawa, ul. Jana Olbrachta 94B.

2. GUGiK, Centrum Zarządzania ASG-EUPOS w Katowicach, ul. Graniczna 29, 40-017 Katowice w zakresie centrum zapasowego dla systemu KSZBDOT – oczekiwane utrzymanie głównie oparte na zdalnym dostępie do środowiska.

7.6 Aplikacje dedykowane

1. Edytor metadanych

Edytor Metadanych jest jednym z produktów Projektu Geoportal 2, wytworzonym jako jedno z narzędzi do harmonizacji. Aplikacja umożliwia przygotowanie nowych plików metadanych, edycję istniejących oraz przeprowadzenie walidacji (z wykorzystaniem narzędzia Walidatora metadanych). Aplikacja działa w trybie online, jest dostępna z poziomu przeglądarki internetowej. Aplikacja przeznaczona jest dla podmiotów zajmujących się przetwarzaniem plików metadanych na potrzeby publikacji plików metadanych. Użytkownikami aplikacji są jednostki organizacyjne GUGiK i CODGiK oraz podmioty zewnętrzne.

2. Walidator metadanych

Walidator metadanych jest jednym z produktów Projektu Geoportal 2, wytworzonym jako jedno z narzędzi do harmonizacji. Aplikacja umożliwia zwalidowanie plików metadanych, tzn. sprawdzenie ich poprawności i zgodności z wybranym profilem metadanych (m.in. profil INSPIRE, profile dla danych dziedzinowych np. EMUiA, NMT). Aplikacja działa w trybie online, jest dostępna z poziomu przeglądarki internetowej. Aplikacja przeznaczona jest dla podmiotów zajmujących się przetwarzaniem plików metadanych na potrzeby publikacji plików metadanych. Użytkownikami aplikacji są jednostki organizacyjne GUGiK i CODGiK oraz podmioty zewnętrzne. Aplikacja jest zintegrowana z Edytorem metadanych (Edytor metadanych wykorzystuje Walidator podczas walidacji wytworzonych plików metadanych).

3. Aplikacja EMUiA

Aplikacja EMUiA została wytworzona w ramach Projektu TERYT 2 i została rozbudowana w ramach Projektu TERYT 3 (obecnie funkcjonuje w postaci 2 instancji produkcyjnych). Aplikacja dostępna jest z poziomu przeglądarki internetowej, przeznaczona jest dla gmin i umożliwia im prowadzenie ewidencji miejscowości, ulic i adresów zgodnie z obowiązującymi przepisami. Aplikacja umożliwia prowadzenie ewidencji, aktualizację danych, a także obsługę wniosków związanych z prowadzeniem ewidencji (np. nadawanie numeru porządkowego).

4. GEOPORTAL

System Geoportal wytworzony został w ramach Projektu Geoportal.gov.pl i rozwijany jest w ramach Projektu Geoportal 2. System Geoportal pełni rolę brokera INSPIRE, krajowego i branżowego, zapewniając dostęp do zbiorów i usług danych przestrzennych. Na system Geoportal składają się m.in. szyna usług SOA, narzędzia do zarządzania publikacją danych i usług, aplikacja zarządzania treścią witryny Geoportal, narzędzia do zarządzania warstwą prezentacji, narzędzia do gromadzenia, zarządzania i publikowania danych dziedzinowych, aplikacje do monitorowania i sprawozdawczości i inne.

5. System Zarządzania K-GESUT

System Zarządzania Krajową bazą danych Geodezyjnej Sieci Uzbrojenia Terenu (System Zarządzania K-GESUT) to system informatyczny wytworzony w ramach Projektu K-GESUT. SZ K-GESUT to system teleinformatyczny, który służy do tworzenia, prowadzenia i udostępniania baz danych K-GESUT. Bazy danych K-GESUT zasilane są danymi z baz GESUT prowadzonych przez starostów powiatowych. Użytkownikami systemu są pracownicy CODGiK i GUGiK.

6. KSZBDOT

Krajowy System Zarządzania Bazą Danych Obiektów Topograficznych (KSZBDOT) wytwarzany jest w ramach Projektu GBDOT). KSZBDOT to system teleinformatyczny, który służy do tworzenia, prowadzenia i udostępniania baz danych: obiektów topograficznych i obiektów ogólnogeograficznych oraz zarządzania bazami danych, z których powstaną standardowe opracowania kartograficzne. Użytkownikami systemu są pracownicy WODGiK, CODGiK i GUGiK. System działa w trybie online, jest dostępny z poziomu przeglądarki internetowej.

7. Moduł SDI

Moduł SDI to oprogramowanie służące do tworzenia węzłów infrastruktury informacji przestrzennej, wytworzone w ramach Projektu Geoportal 2. Moduł SDI umożliwia przechowywanie, zarządzanie

oraz udostępnianie danych i metadanych będących w dyspozycji dysponenta danych., a także wymianę danych z innymi użytkownikami wykorzystującymi Moduł SDI. Oprogramowanie Modułu SDI jest przekazywane przez GUGiK nieopłatnie jednostkom administracji rządowej i samorządowej na podstawie porozumienia zawieranego pomiędzy podmiotem a Głównym Geodetą Kraju.

Obecne w infrastrukturze SIG na potrzeby użytkowników gminnych zostało stworzonych i udostępnionych do użytkowania (hostowanych) ponad 300 instancji węzłów wykorzystujących oprogramowanie Modułu SDI. Wszystkie instancje są niezależne biznesowo i w dużej mierze technologicznie, w szczególności w warstwie oprogramowania standardowego.

8. System do generalizacji TOPO

System do generalizacji TOPO to aplikacja wytwarzana w ramach Projektu GBDOT. System do generalizacji TOPO służy do generowania z utworzonej w ramach projektu GBDOT bazy danych obiektów topograficznych (BDOT10k) bazy danych obiektów ogólnogeograficznych (BDOO). Użytkownikami systemu będą pracownicy CODGiK i GUGiK.

9. SZNMT

System Zarządzania Numerycznym Modelem Terenu (SZNMT) wytwarzany jest w ramach Projektu ISOK. System umożliwia zarządzanie danymi fotogrametrycznymi (m.in. zobrazowania lotnicze i satelitarne, ortofotomapa, dane wysokościowe i metadane dla ww. danych), a także wspiera kontrole i udostępnianie danych fotogrametrycznych. Użytkownikami systemu są pracownicy GUGiK i CODGiK.

10. SZPRG

System Zarządzania Państwowym Rejestrem Granic i Powierzchni Jednostek Podziałów Terytorialnych Kraju (SZPRG) został wytworzony w ramach Projektu TERYT 2 i został rozbudowany w ramach Projektu TERYT 3.System umożliwia prowadzenie rejestru granic jednostek podziału terytorialnego w zakresie zgodnym z rozporządzeniem Rady Ministrów w sprawie państwowego rejestru granic i powierzchni jednostek podziałów terytorialnych kraju oraz prowadzenie ewidencji adresów wraz ich lokalizacją przestrzenną. SZPRG zasilany jest m.in. danymi z ewidencji miejscowości, ulic i adresów, prowadzonymi przez gminy. Użytkownikami SZPRG są pracownicy GUGiK i CODGiK.

11. Uniwersalny Moduł Mapowy – SDI+

Uniwersalny Moduł Mapowy to jeden z produktów Projektu Geoportal 2. Do uzyskania pełni funkcjonalności Uniwersalnego Modułu Mapowego wymagane jest wykorzystanie Modułu SDI. UMM to zestaw narzędzi analityczno-raportowych, które umożliwiają wykonywanie analiz na danych

zgromadzonych w bazach Modułu SDI, a także wizualizację i udostępnianie wyników. Narzędzie posiada dedykowane funkcjonalności dla dyspozytorów i analityków, a także dla użytkowników urządzeń mobilnych. Użytkownikami UMM są przede wszystkim służby ratunkowe wykorzystujące narzędzie do prowadzenia działań operacyjnych.

12. ZSIN

Zintegrowany System Informacji o Nieruchomościach (ZSIN) to system informatyczny budowany przez GUGiK w ramach Projektu ZSIN. W ramach Projektu stworzone zostało m.in. Centralne Repozytorium Kopii Zbiorów Danych EGiB – rejestr zawierający zintegrowane dla całego kraju dane z ewidencji gruntów i budynków, a także rozbudowane zostały narzędzia umożliwiające prowadzenie ewidencji w starostwach powiatowych. Budowa ZSIN zakładała migrację i rozbudowę Systemu IPE, który stanie się centralnym komponentem ZSIN, będzie pełnił rolę brokera usług. Punktem dostępowym do usług dla zewnętrznych systemów dziedzinowych oraz lokalnych systemów do prowadzenia EGiB jest Szyna usług ZSIN, której rolę pełni rozbudowana w ramach Projektu Szyna usług.

13. PRPOG

W części centralnej państwowego zasobu geodezyjnego i kartograficznego prowadzony jest państwowy rejestr podstawowych osnów geodezyjnych, grawimetrycznych i magnetycznych (PRPOG) zgodnie ze standardem określonym w rozporządzeniu Ministra Administracji i Cyfryzacji z dnia 14 lutego 2012 r. w sprawie osnów geodezyjnych, grawimetrycznych i magnetycznych (Dz. U. z 2012 r., poz. 352). Zasadniczą częścią PRPOG jest baza danych zawierająca informacje, zbiory danych i obserwacji (także archiwalne) i opracowania wyników obserwacji, dotyczące punktów 1 i 2 klasy podstawowej osnowy geodezyjnej oraz podstawowej osnowy grawimetrycznej i magnetycznej. Utrzymanie, aktualizacja i udostępnianie bazy danych PRPOG odbywa się poprzez oprogramowanie zarządzające pod nazwą „System państwowego rejestru podstawowych osnów geodezyjnych, grawimetrycznych i magnetycznych (system PRPOG).

14. PZGiK

System przeznaczony do obsługi centralnej części państwowego zasobu geodezyjnego i kartograficznego składa się z dwóch podstawowych modułów:
- część portalowa umożliwiająca klientom zewnętrznym złożenie wniosku, dokonanie opłaty oraz pobranie danych, zawiera także funkcjonalności dotyczące zarządzania kontami użytkowników i zarządzania kontaktami z klientami

- część wewnętrzna, stanowiąca rozbudowany system kancelaryjny, umożliwiający, poza podstawowymi funkcjonalnościami obsługi spraw i dokumentów, także integrację z systemami dziedzinowymi, w których gromadzone się dane państwowego zasobu geodezyjnego kartograficznego a także obsługę wymaganych przepisami rejestrów i ewidencji.

7.7 Usługi biznesowe

Szacowana liczba usług biznesowych – 60. Przykładowe usługi biznesowe:

1. Usługa wyszukiwania danych przestrzennych,
2. Usługa przeglądania danych przestrzennych,
3. Usługa pobierania danych przestrzennych,
4. Usługi przekształcania danych przestrzennych,
5. Usługa uruchamiania usług danych przestrzennych,
6. Usługa sprzedaży danych przestrzennych,

7.8 Serwerownia

7.8.1 Lokalizacja Warszawa

Obecnie serwerownia zlokalizowana w CODGiK przy ul. Olbrachta 94B w Warszawie składa się z jednego pomieszczenia. Zamawiający planuje rozbudowę serwerowni o dodatkowe pomieszczenie umożliwiające zainstalowanie sprzętu w ok. 12 szafach, zlokalizowane w tym samym budynku. Planowany termin zakończenia prac dostosowania pomieszczenia – IV kwartał 2017 r.

Pomieszczenie wyposażone będzie w niezbędną infrastrukturę zasilania, chłodzącą, gaszenia, okablowanie strukturalne oraz szafy rack. Zamawiający zapewnia redundantne przyłącza internetowe w lokalizacji Warszawa oraz łącze punk-punkt Warszawa-Katowice.

Pomieszczenia będą połączone ze sobą okablowaniem infrastrukturalnym światłowodowym i miedzianym (LAN/SAN), którego długość nie przekracza 100m.

7.8.2 Lokalizacja Katowice

Obecnie serwerownia zlokalizowana w Katowicach udostępnia miejsce dodatkowo na 1 szafę (42U) (poza zainstalowanymi obecnie urządzeniami). Przeznaczeniem lokalizacji jest zdalne przechowywanie kopii zapasowej. Zasilanie nie posiada gwarancji podtrzymania.

7.9 Warstwa aplikacyjna

Obecna infrastruktura warstwy aplikacyjnej składa się z 25 serwerów Blade (posiadających łącznie 13TB pamięci operacyjnej RAM, 350 rdzeni Intel, serwery bezdyskowe), umiejscowionych

w czterech klatkach Blade. Urządzenia pod względem parametrów pamięci i procesora nieznacznie się różnią, jednak wszystkie są oparte na architekturze x86. Powyżej wymienione urządzenia są wykorzystywane jako elementy chmury obliczeniowej opartej o platformę wirtualizacyjną VMware vSphere Enterprise Plus.

Do ochrony antywirusowej środowiska wirtualizacyjnego wykorzystywane jest oprogramowanie Trend Micro Deep Security.

Obecnie w środowisku wirtualizacyjnym (VMware) funkcjonuje ok. 870 maszyn wirtualnych (sumarycznie środowiska produkcyjne i testowe), opartych o systemy operacyjne: Windows Server (Active Directory), Linux – Centos.

7.10 Warstwa szyny usług

Warstwa składa się z czterech serwerów typu blade, na których jest uruchomione rozwiązanie wirtualizacyjne Oracle VM, a w ramach niego oprogramowanie szyny usług SOA Oracle Service Bus 12c (Usługi infrastrukturalne np.: SAML WebSSO, usługa uwierzytelniania grubego klienta, usługa monitorowania) oraz szyna usług OGC - iMapESB (usługi przestrzenne OGC np.: WMS, WFS, CSW) uruchomiona w klastrze VMware. Dostawcą tożsamości dla obu szyn jest LDAP.

7.11 Warstwa bazy danych

Infrastruktura warstwy bazy danych oparta jest o skonsolidowane rozwiązanie sprzętowo – programowe – Exadata Half Rack X2. Rozwiązanie składa się z serwerów (4 węzły bazodanowe (łącznie 1134 GB RAM i 48 Rdzeni CPU x86)) i sprzętu typu storage (360 TB pojemności użytecznej), który jest zarządzany w jednolity sposób za pomocą dedykowanego oprogramowania zintegrowanego z oprogramowaniem bazodanowym. Oprogramowanie zapewnia funkcjonalności typowej relacyjnej bazy danych i jest wzbogacone o funkcjonalności umożliwiające elastyczne zarządzanie dedykowaną infrastrukturą sprzętową. Wykorzystywane są następujące opcje Oracle Database Enterprise Edition: RAC, Spatial, Partitioning, Diagnostic Pack, Tuning Pack.

Obecnie w środowisku bazy danych istnieje ok. 60 instancji baz danych.

7.12 Warstwa storage i magazyny danych

Warstwa storage składa się z macierzy dyskowej - dostęp blokowy oraz NAS. Wśród urządzeń wyróżniamy główne elementy takie jak:

- IBM SoNAS 2851-RXA – Usługę dostępu sieciowego NAS (głównie CIFS, NFS, FTP), pojemność użyteczna - 560 TB;

- IBM Storwize V7000 wraz z półkami rozszerzającymi, usługę dostępu blokowego (dla maszyn wirtualnych oraz bezdyskowych serwerów Blade), pojemność użyteczna – 120 TB.

7.13 Warstwa sieci

Warstwa sieci składa się z urządzeń sieciowych umożliwiających działanie sieci LAN i sieci SAN.

Obecna infrastruktura to:

1. Juniper SRX3400 Firewall Klaster – 2 szt;
2. NLB F5 BIG-BT-5250V – 2 szt;
3. Terminator VPN Cisco 5510 K9 – 1 szt;
4. Switche LAN (Juniper EX 4200-48T – 4 szt., EX2200-24T – 4 szt.)
5. Switche SAN (IBM System Storage SAN48B-5) - 2szt;
6. Switch LAN (IBM System Networking RackSwitch G8124E) - 1szt;
7. HSM (Thales nShield Connect 1500) 2szt;
8. Klaster Router (Juniper J6350) 2szt.

7.14 Warstwa dostępowa

Łącza:

- Dwa niezależne łącza dostępowe do Internetu (500 Mbps, 300 Mbps);
- Wydzielone połączenie do sieci OST 112;
- Łącze point-to-point (Katowice – Warszawa) o przepustowości 512 Mbps.

Metody dostępu:

- Dostęp za pomocą VPN CISCO Client z lokalną usługą po http;
- Dostęp przez przeglądarkę www z szyfrowaniem (https);
- Tunel IPSec (VPN Poin To Point);
- SSL VPN F5 z lokalną usługą po http.

7.15 Środowisko backupowe

Środowisko backupowe złożone jest z urządzenia do deduplikacji EMC DataDomain DD2500, biblioteki taśmowej TS3310 wraz z taśmami magnetycznymi LTO oraz serwera zarządzania backupem.

Rozwiązanie sprzętowe zarządzane jest przez oprogramowanie do backupu danych Veritas NetBackup. Oprogramowanie jest zainstalowane na serwerze do zarządzania backupem oraz w ramach środowiska aplikacyjnego.

Środowisko backupowe ma za zadanie wykonywanie kopii zapasowych z baz danych, warstwy aplikacyjnej , NAS, maszyn wirtualnych oraz szyny usług.

Elementem składowym środowiska backupowego jest Centrum Zapasowe w Katowicach, spełniające rolę miejsca przechowywania danych (maszyn wirtualnych i baz danych) w dodatkowej lokalizacji, innej niż Centrum Podstawowe w Warszawie. Środowisko Centrum Zapasowego w Katowicach składa się z analogicznych rozwiązań jak w Centrum Podstawowym (serwer zarządzania backup z oprogramowaniem Symantec NetBackup, biblioteka taśmowa i deDuplikacja EMC DataDomain DD2500).

7.16 Środowisko monitoringu

W ramach warstwy wykorzystywane jest oprogramowanie do monitorowania – Nagios, Centreon zbierające dane z infrastruktury oraz Nagvis wizualizujący zebrane dane.

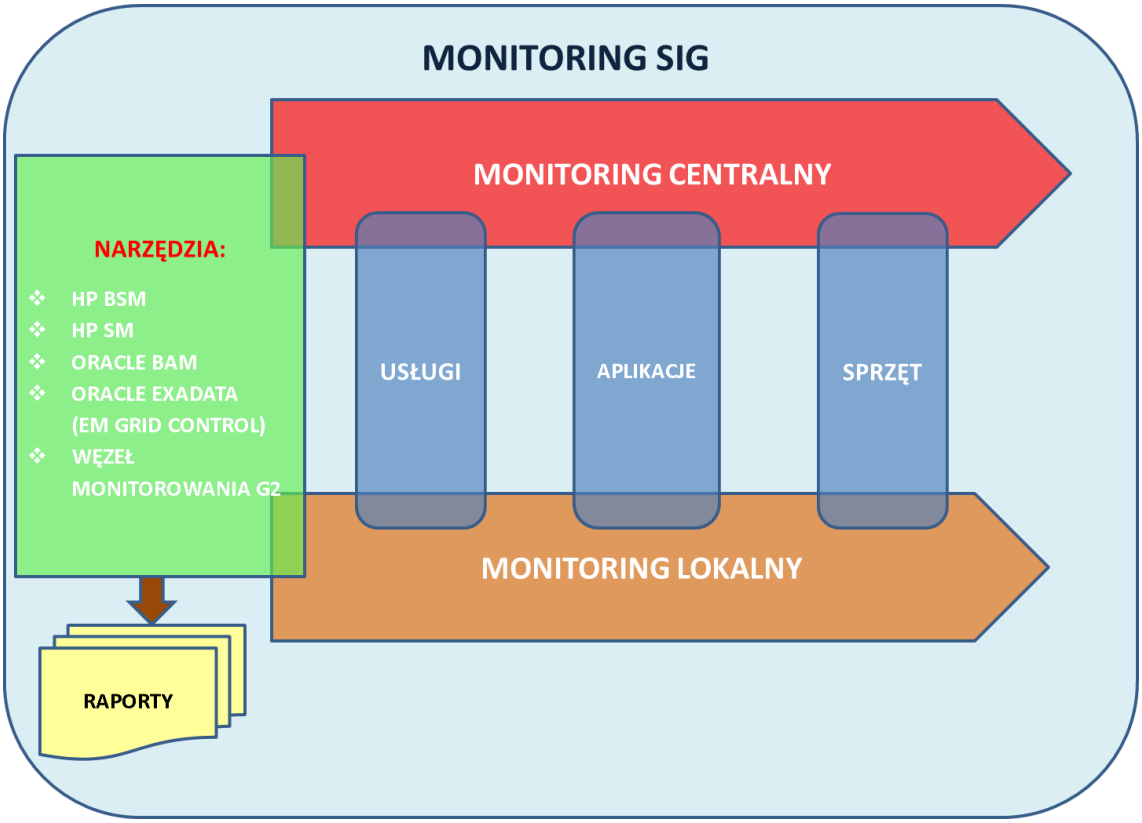
W ramach warstwy wykorzystywane są także inne metody zbierania informacji o parametrach działania systemu, m.in. mechanizmy wbudowane w oprogramowanie do wirtualizacji VMware ESX, mechanizmy wbudowane w urządzenia sieciowe.

System monitoringu HP w oparciu o wybrane elementy (HP Real User Monitor Engine, HP SiteScope 11.23, HP Performance Manager, HP Network Node Manager, HP BSM)

Do zbierania informacji o parametrach działania poszczególnych elementów infrastruktury wykorzystywane są również mechanizmy wbudowane w posiadane oprogramowanie, m.in. oprogramowanie do wirtualizacji VMware ESX, mechanizmy wbudowane w urządzenia sieciowe.

Ogólna koncepcja systemu monitorowania SIG została przedstawiona poniżej.

Model systemu monitoringu SIG powinien być oparty na posiadanych i planowanych narzędziach, które pozwolą na spojrzenie zarówno globalne na całość zasobów, zwłaszcza priorytetowych – monitoring centralny, jak i na spojrzenie bardziej szczegółowe na wszystkie zasoby i kluczowe parametry wymienione w rozdziale 12.4.7. Koncepcję przedstawiono na poniższym schemacie.



Schemat.1. Model logiczny rozwiązania – schemat

GUGiK jest w posiadaniu m.in. następujących narzędzi do monitorowania:

1. HP BSM – monitorowanie na poziomie centralnym i lokalnym (obszar sprzętowy, usługowy, aplikacyjny)
   Narzędzia w ramach pakietu:
   - HP Business Process Monitor – głównie badanie dostępności i wydajności aplikacji oraz badanie poprawności działania usługi/systemu z punktu widzenia użytkownika;
   - HP Real User Monitor – badanie ruchu sieciowego generowanego przez użytkowników oraz aplikacje, a także dostępności wybranych urządzeń/aplikacji w czasie rzeczywistym;
   - HP Business Service Manager – platforma integrująca pozostałe rozwiązania firmy HP z rodziny BTO (Business Technology Optimization);

- HP Operations Management for Windows – produkt dla platformy Windows, do zarządzania dostępnością infrastruktury, zdarzeniami i wydajnością przy użyciu agentów i reguł korelacji zdarzeń;
- HP Operations Agent – agent, składający się z komponentu operacyjnego i wydajnościowego, do monitorowania procesów systemu i aplikacji oraz reakcji na zdarzenie (zdefiniowane procedury naprawcze) a także monitorowanie i raportowanie wydajności systemu;
- HP Performance Manager – narzędzie do prezentacji wydajności z węzłów z agentami;
- History Messages – narzędzie autorskie firmy Devoteam, do przechowywania i wyszukiwania historycznych komunikatów z systemu monitorowania;
- HP SiteScope – narzędzie skanujące system BSM;
- HP Smart Plug-In for System Infrastructure – dodatki programowe do monitorowania systemów operacyjnych;
- HP Smart Plug-In for Virtualization Infrastructure – dodatki programowe do monitorowania hostów wirtualanych;
- HP Smart Plug-In for Oracle DataBase – dodatki programowe do monitorowania baz danych Oracle;

Uwaga. Dla sprawnego uruchomienia/działania monitorowania SIG przy wykorzystaniu narzędzi z grupy HP BSM niezbędna jest odpowiednia konfiguracja systemu względem monitorowanych zasobów oraz rekonfiguracja w przypadku istotnych zmian we właściwościach zasobów (np. zmiana adresu aplikcji, portu itd.)

2. HP Service Manager – monitorowanie na poziomie lokalnym i centralnym poziomu zarządzania usługami informatycznymi w organizacji zgodnie z ITIL dla procesów :
    - Zarządzanie incydentami,
    - Zarządzanie problemami,
    - Zarządzanie konfiguracją,
    - Zarządzanie zmianami,
    - Zarządzanie poziomem usług,
    - Zarządzanie wiedzą,
    - Zarządzanie zasobami,
    - Zarządzanie wersjami i wdrożeniami,
    - Weryfikacji i testowanie usług.

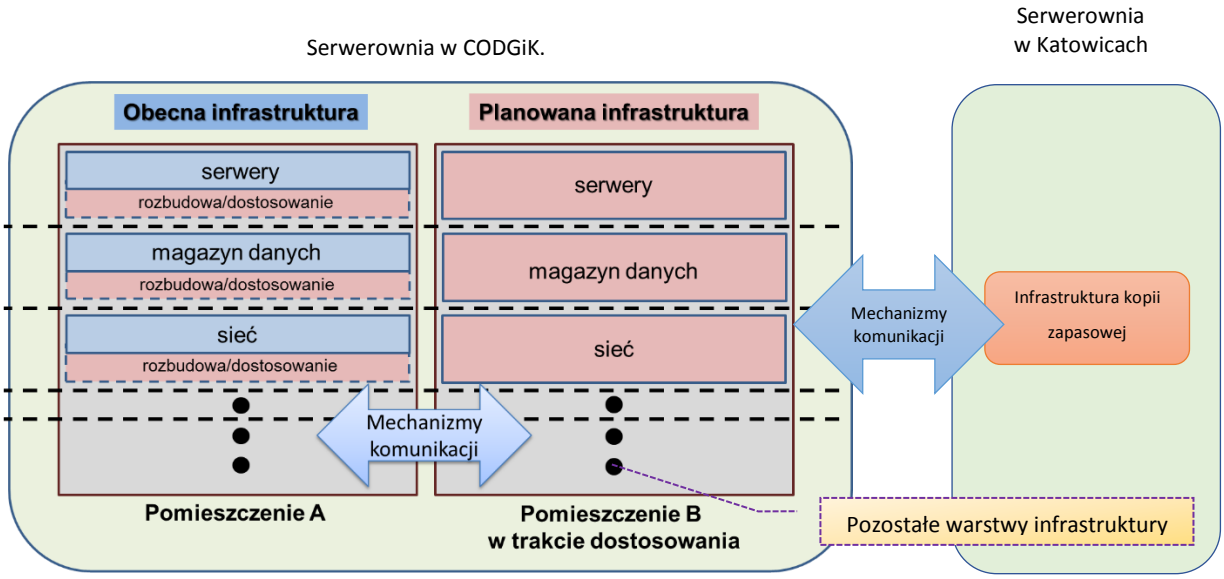
3. Oracle Business Activity Monitoring (BAM) – narzędzie do monitorowania na poziomie lokalnym, przede wszystkim parametrów na poziomie szyny usług i pozostałych rozwiązań oraclowych;
4. Wewnętrzne mechanizmy monitorowania Zintegrowanego środowiska bazodanowego – monitorowanie na poziomie lokalnym, przede wszystkim Zintegrowany storage bazodanowy Oracle oraz hostowane bazy danych oraz dostępne zasoby sprzętowe na nim;

5. Węzeł monitorowania G2 – monitoring usług wyszukiwania, pobierania i transformacji realizowanych przez zdefiniowane węzły Infrastruktury Informacji Przestrzennej poprzez symulację zachowań użytkownika systemu. Aplikacja zgodnie z założeniami służyć będzie do weryfikacji informacji raportowych Głównego Geodety Kraju zgodnie z dyrektywą INSPIRE oraz do weryfikacji informacji o monitorowaniu węzła centralnego a także powinna umożliwiać automatyczne powiadamianie administratora o wykrytych problemach.

8 Ogólna koncepcja docelowego rozwiązania

Poniższy diagram przedstawia wizję docelowego rozwiązania w zakresie infrastruktury techniczno-programowej.

Rysunek 19 Wizja docelowego rozwiązania



W ramach postępowania zakładane jest dostarczenie środowiska, które umożliwi uruchomienie systemów informatycznych na wirtualnej platformie systemowej, a zastosowane rozwiązania umożliwią docelowo ich integrację w ramach prywatnej chmury obliczeniowej administracji publicznej. Zastosowanie technologii chmury obliczeniowej w realizacji projektu dostarczy horyzontalnych w skali administracji rozwiązań w zakresie optymalizacji wykorzystania infrastruktury, w szczególności poprzez udostępnienie ponad resortowych rozwiązań.

Podstawową cechą planowanej infrastruktury ma być zapewnienie pełnej redundancji funkcjonalnej dla posiadanego środowiska, oraz rozszerzenie jej funkcjonalności głównie poprzez zwiększenie mocy obliczeniowej i pojemności. Budowa infrastruktury nie wyklucza możliwości modyfikacji w obecnie posiadanej infrastrukturze w celu zapewnienia wyżej wymienionych funkcjonalności. Każdy element infrastruktury sprzętowej ma być redundantny.

Centrum danych w Katowicach ma pełnić funkcję zdalnego centrum przechowywania kopii zapasowych danych. Replikacja odbywać się będzie przy pomocy dedykowanego łącza punkt-punkt.

Rozwiązanie objęte będzie usługą utrzymania opisaną w punktach 11. Utrzymanie oraz 12. Zakres prac Utrzymaniowych.

8.1 Planowany poziom dostępności infrastruktury

Dostarczona oraz skonfigurowana infrastruktura w ramach przedmiotowego postępowania w połączeniu z elementami infrastruktury posiadanej przez Zamawiającego w całości, ma zapewnić minimalny poziom dostępności w poszczególnych warstwach infrastruktury opisany w poniższej tabeli.

RTO	RPO	Minimalny poziom dostępności w miesiącu	Minimalny poziom dostępności w roku
Poniżej 4h	Poniżej 4h	99,5 %	99,5%

9 Dostawa infrastruktury i oprogramowania

Dostarczone w ramach postępowania poszczególne elementy infrastruktury muszą spełniać poniższe wymagania:

1. Wszystkie oferowane urządzenia muszą być fabrycznie nowe (na dzień dostawy urządzenia nie mogą być starsze niż 6 miesięcy od daty produkcji oraz nie mogą być używane).
2. Wszystkie oferowane urządzenia muszą być wyprodukowane zgodnie z normą jakości ISO 9001:2000 lub normą równoważną.
3. Urządzenia i ich komponenty muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
4. Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych.
5. Oferowane urządzenia muszą pochodzić z oficjalnego kanału dystrybucji producenta na terenie Unii Europejskiej, a gwarancja (wsparcie techniczne) musi pochodzić od producenta i być świadczona przez sieć serwisową producenta na terenie Polski.
6. Dla wszystkich dostarczanych urządzeń Wykonawca dostarczy odpowiednią ilość, o odpowiednich parametrach: wkładek optycznych, kabli zasilających, kabli FC, kabli Ethernet, kabli optycznych Ethernet 10-40 Gbps oraz innych akcesoriów, niezbędnych do przeprowadzenia prawidłowej instalacji urządzeń.
7. Na dzień złożenia oferty oferowane urządzenia nie mogą być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.

Dla wyspecyfikowanej infrastruktury oraz oprogramowania, Wykonawca zobowiązany jest do udzielenia niewyłącznej licencji (na oprogramowanie) Zamawiającemu lub przeniesie na Zamawiającego niewyłączne uprawnienia licencyjne na czas nieoznaczony, tj. nieograniczony w czasie na korzystanie z dostarczonego oprogramowania.

Procedura przekazania oraz odbioru przedmiotu dostawy (infrastruktura sprzętowa wraz z oprogramowaniem) odbywać się będzie na poniższych zasadach:

1. Wykonawca zobowiązany jest przed przeprowadzeniem dostawy powiadomić (pisemnie lub poprzez wiadomość e-mail) Zamawiającego o planowanej dostawie (lub jej części), na co najmniej 3 dni robocze przed jej przeprowadzeniem.
2. Wykonawca zobowiązany jest przeprowadzić dostawę przedmiotu dostawy w godzinach uzgodnionych z Zamawiającym.

3. Po dostarczeniu przez Wykonawcę infrastruktury sprzętowej oraz oprogramowania podpisywany jest przez Strony, Protokół Odbioru Ilościowego stanowiący Załącznik nr 5, stwierdzający faktyczną ilość sztuk dostarczonej infrastruktury sprzętowej oraz oprogramowania.
4. Po zainstalowaniu i podstawowym skonfigurowaniu wszystkich dostarczonych elementów infrastruktury, w stopniu umożliwiającym potwierdzenie spełnienia wymagań określonych w OPZ, Zamawiający zweryfikuje w terminie nie przekraczającym 14 dni, czy dostarczony przedmiot dostawy jest zgodny z OPZ. Po weryfikacji podpisywany jest Protokół Odbioru Dostawy.

Szczegółowe warunki wsparcia technicznego dla wszystkich wyspecyfikowanych w rozdziale 9 elementów infrastruktury:

1. Wykonawca udzieli Zamawiającemu nieodpłatną usługę wsparcia technicznego na dostarczoną infrastrukturę sprzętową.
2. Okres usługi wsparcia technicznego zarówno dla sprzętu i oprogramowania będzie obowiązywał dla poszczególnych elementów infrastruktury - od dnia zainstalowania poszczególnych elementów infrastruktury, do dnia podpisania przez Zamawiającego Protokołu Odbioru Dostawy oraz od dnia podpisania przez Zamawiającego Protokołu Odbioru Dostawy przez okres zgodny z ofertą Wykonawcy - „Czas Trwania Wsparcia Technicznego”.
3. Usługa wsparcia technicznego obejmuje zobowiązanie Wykonawcy do terminowego usuwania wad i usterek sprzętu komputerowego oraz innych elementów stanowiących przedmiot dostawy.
4. Prawo do pobierania i instalowania aktualizacji firmware oraz oprogramowania systemowego, udostępnianego przez producenta sprzętu, w czasie trwania usługi wsparcia technicznego.
5. Prawo do pobierania i instalowania aktualizacji sygnatur bezpieczeństwa, udostępnianych przez producenta sprzętu, w czasie trwania usługi wsparcia technicznego.
6. Wykonawca zobowiązuje się, iż w okresie usługi wsparcia technicznego, czas reakcji na zgłoszoną wadę lub usterkę, nastąpi nie później niż w ciągu 1 dnia od momentu zgłoszenia wady lub usterki.
7. Wykonawca zobowiązuje się do dokonania bezpłatnej naprawy dostarczonego sprzętu, w ciągu 1 dnia licząc od dnia, w którym dokonano zgłoszenia wady lub usterki, danego urządzenia.
8. Naprawa, zostanie dokonana w miejscu, w którym sprzęt został zainstalowany.
9. W przypadku braku możliwości wykonania przez Wykonawcę, naprawy w miejscu i w terminie, o którym mowa powyżej, Wykonawca zobowiązuje się dostarczyć i odpowiednio

skonfigurować oraz zainstalować takie samo urządzenie wolne od wad i zapewni jego prawidłowe działanie. Po uruchomieniu urządzenia zastępczego zostanie spisany protokół wymiany urządzenia.

10. W przypadku uszkodzenia nośnika danych w stopniu takim, że nie będzie możliwa jego dalsza eksploatacja, Wykonawca zobowiązany jest do wymiany uszkodzonego nośnika danych na nowy. Uszkodzony nośnik danych pozostaje u Zamawiającego.
11. Wykonawca pokrywa wszelkie koszty związane z naprawami.
12. Zamawiający ma prawo do dokonywania rozbudowy infrastruktury sprzętowej, zgodnie z dokumentacją techniczną producenta, przez wykwalifikowanych pracowników, bez utraty wsparcia technicznego. Wykonawca nie ponosi odpowiedzialności za uszkodzenia przedmiotu Umowy powstałe z winy Zamawiającego.

Wykonawca zobowiązany jest dostarczyć następujące elementy infrastruktury:

W wypadku wystąpienia w niniejszym Opisie Przedmiotu Zamówienia zastrzeżonych nazw własnych producentów lub produktów, zgodnie z art. 29 ust. 3 ustawy – Prawo Zamówień Publicznych, dopuszcza się oferowanie produktów w pełni równoważnych do wymaganych przy pełnym zagwarantowaniu przez Wykonawcę zachowania całkowitej projektowanej funkcjonalności.

9.1 Obudowa blade (klatka) – 2 szt.

Produkt musi spełnić następujące wymagania:

9.1.1 Wymagania ogólne

ID	Wymaganie
1	Obudowa, o wysokości maksymalnie 10U, musi być przystosowana do montażu w szafie typu rack 19”, umożliwiająca obsadzenie minimum 16 serwerów dwuprocesorowych bez konieczności rozbudowy o kolejne elementy sprzętowe.
2	Możliwość umieszczania w ramach pojedynczej obudowy wszystkich typów serwerów blade obecnych w ofercie danego producenta.
3	Sposób agregacji/wyprowadzeń sygnałów LAN dla pojedynczej obudowy. Minimum dwa przełączniki LAN. Urządzenia te muszą umożliwiać agregację połączeń LAN w infrastrukturze blade i muszą umożliwiać wyprowadzenie sygnałów LAN z infrastruktury z zachowaniem redundancji połączeń. Każdy z modułów musi posiadać minimum 16 wewnętrznych portów 20Gb lub minimum 32 wewnętrzne porty 10Gb do serwerów (sumaryczne pasmo portów wewnętrznych pojedynczego modułu LAN do serwerów, musi wynosić minimum 320Gb).

ID	Wymaganie
	Każdy z modułów musi posiadać porty zewnętrzne: • Minimum 4 porty 40Gb • Minimum 4 portów 10Gb Sumaryczna przepustowość portów zewnętrznych (porty 40Gb oraz porty 10Gb, nie dopuszcza się samych portów 40Gb) musi wynosić minimum 200Gb dla pojedynczego modułu LAN. Dostarczone moduły należy obsadzić odpowiednimi do prędkości portów wkładkami. Wszystkie dostępne, fizyczne porty (wewnętrzne oraz zewnętrzne) każdego modułu LAN (niezależnie od minimalnej wymaganej ilości portów) muszą być aktywne i gotowe do obsługi ruchu sieciowego bez konieczności dokupowania elementów sprzętowych lub dodatkowych licencji. Należy dostarczyć wszystkie niezbędne licencje do aktywacji wszystkich portów urządzeń.
4	Każda obudowa musi posiadać minimum dwa moduły typu switch 16Gb Fibre-Channel wyprowadzające sygnały z minimum 2 portów FC na serwerach. Urządzenia te muszą umożliwiać agregację połączeń SAN w infrastrukturze blade i muszą umożliwiać wyprowadzenie sygnałów SAN z infrastruktury z zachowaniem redundancji połączeń. Każdy moduł musi posiadać minimum 8 zewnętrznych portów obsadzonych modułami 16Gb SFP+ SW. Wszystkie dostępne, fizyczne porty każdego modułu Fibre-Channel muszą być aktywne i gotowe do obsługi ruchu sieciowego SAN bez konieczności dokupowania elementów sprzętowych lub dodatkowych licencji. Każdy moduł powinien umożliwiać (posiadać licencje): • ISL Trunking • Fabric Watch • Extended Fabric • Zaawansowane zarządzanie wydajnością
5	Możliwość przydzielania adresów MAC i WWN predefiniowanych przez producenta rozwiązania blade dla poszczególnych wnęk na serwery w obudowie. Przydzielenie adresów musi powodować zastąpienie fizycznych adresów kart Ethernet i Fibre-Channel na serwerze. Musi istnieć także możliwość przenoszenia przydzielonych adresów pomiędzy wnękami w obudowie. Funkcjonalność ta może być realizowana zarówno poprzez moduły LAN i SAN w infrastrukturze jak i poprzez dodatkowe oprogramowanie producenta serwerów blade. Dodatkowo dla sieci LAN musi istnieć możliwość stworzenia niezależnych połączeń VLAN tak aby między wydzielonymi sieciami nie było komunikacji. Wymagana jest możliwość boot'owania systemów operacyjnych zainstalowanych na poszczególnych serwerach blade bezpośrednio z macierzy w środowisku SAN. Wymagane wszystkie niezbędne licencje na opisaną funkcjonalność dla całej infrastruktury blade. W przypadku sieci LAN, musi istnieć możliwość określenia pasma przepustowości pojedynczego portu LAN na serwerze od 100Mb/s do 10Gb/s.
6	Każda z obudów na serwery wyposażona w zestaw redundantnych wentylatorów (typ hot plug, czyli możliwość wymiany podczas pracy urządzenia) zapewniających chłodzenie dla maksymalnej liczby serwerów i urządzeń I/O zainstalowanych w obudowie blade. Wentylatory niezależne od zasilaczy, wymiana wentylatora (wentylatorów) nie może powodować konieczności wyjęcia

ID	Wymaganie
	zasilacza (zasilaczy).
7	Każda z obudów wyposażona w zestaw zasilaczy redundantnych typu Hot Plug. System zasilania zdolny do obsługi awarii połowy z zainstalowanych zasilaczy (dowolne N zasilaczy przy założeniu konfiguracji N + N), wymagane ciągłe dostarczenie mocy niezbędnej do zasilenia maksymalnej liczby serwerów i urządzeń I/O zainstalowanych w obudowie. Procesory serwerów winny pracować z nominalną, maksymalną częstotliwością. Wymiana zasilacza nie może powodować konieczności odłączenia zewnętrznej infrastruktury zasilania (kabla zasilającego), jak również nie może powodować konieczności wyjęcia lub odłączenia wentylatorów (pojedynczego wentylatora lub modułu wentylatorów).
8	Możliwość instalacji switchy w standardzie InfiniBand.
9	Dwa redundantne, sprzętowe moduły zarządzające, moduły typu Hot Plug. Moduł KVM, umożliwiający podłączenie klawiatury, myszy i monitora.
10	Każda z obudów wchodzących w skład infrastruktury musi posiadać identyczną konfigurację sprzętową w zakresie zasilaczy, wentylatorów oraz modułów I/O.
11	Wraz z infrastrukturą blade, należy dostarczyć odpowiednią ilość modułów PDU do prawidłowego, redundantnego podłączenia infrastruktury blade do zasilania w szafach Zamawiającego. PDU muszą spełniać minimalne wymagania: -minimum 32A -minimum dwa redundantne moduły (należy uwzględnić odpowiednią ilość modułów dla redundantnego podłączenia całej infrastruktury blade) -ilość gniazd zapewniająca podłączenie dostarczonej infrastruktury blade

9.1.1 Wymagania dot. Zarządzania klatką blade

12	Podstawowe funkcje: Zdalne włączanie/wyłączanie/restart niezależnie dla każdego serwera
13	Zdalne udostępnianie napędu CD-ROM/DVD/ISO na potrzeby każdego serwera z możliwością bootowania z w/w napędów.
14	Zdalny sposób zarządzania z poziomu przeglądarki internetowej, bez konieczności instalacji specyficznych komponentów programowych producenta sprzętu.
15	W danym momencie musi być niezależny, równoległy dostęp do konsol tekstowych i graficznych wszystkich serwerów w ramach infrastruktury
16	Zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego
17	Automatyzowana konfiguracja sprzętowa każdego serwera niezależnie oraz wielu serwerów równocześnie za pomocą skryptów
18	Zautomatyzowane instalacje systemu operacyjnego z wykorzystaniem mechanizmu PXE (bootowanie z sieci)

19	Zautomatyzowane, personalizowane, zrównoleglone instalacje systemów operacyjnych oraz aplikacji z wykorzystaniem tzw. Plików odpowiedzi dostarczanych przez producenta oprogramowania użytkowego
20	Zautomatyzowane, zrównoleglone kopiowanie środowisk, połączone z natychmiastową personalizacją systemu
21	Zdalna dystrybucja oprogramowania,
22	Automatyczne wykrywanie i identyfikacja urządzeń zainstalowanych w ramach infrastruktury (serwery, obudowy blade, karty zarządzające) i prezentacja infrastruktury w postaci graficznej
23	Monitorowanie utylizacji następujących podzespołów serwera: procesor, pamięć.
24	Licencje na powyższą funkcjonalność na wszystkie serwery blade możliwe do obsadzenia w oferowanej infrastrukturze blade.

9.2 Serwery

9.2.1 Serwery blade – 26 szt.

Produkt musi spełnić następujące wymagania z poniższym założeniem:

6 szt. serwerów blade do zainstalowania w posiadanej przez Zamawiającego obudowie serwerów kasetowych HP BladeSystem c7000 Enclosure o numerze produktu 681844-B2, nr ser. CZJ45101MT1 i modułami komunikacyjnymi Virtual Connect – wolne zatoki na 6 serwerów z 2 CPU każdy.
20 szt. serwerów blade do zainstalowania w dostarczonych obudowach blade.
Każdy z dostarczanych serwerów musi spełniać poniższe wymagania:

9.2.1.1 Wymagania ogólne

ID	Wymaganie
1	Zainstalowane 2 procesory, minimum 14 rdzeni każdy, x86 - 64 Bit osiągające w testach SPECint_rate2006 wynik nie gorszy niż 1290 punktów w konfiguracji dwuprocesorowej.
2	Zainstalowane 1TB RAM DDR4 Registred DIMMs lub LoadReduces DIMM w modułach min. 64GB. Minimum 16 slotów na pamięć. Możliwość rozbudowy do 1.5TB RAM.
3	Minimum jeden wewnętrzny port USB umożliwiający instalację pamięci Flash.
4	Minimum 2 sloty PCI-Express x8 (szybkość slotu).
5	Dwa Interfejsy SAN FC 16Gb.
6	Minimum 2 Interfejsy sieciowe 20GbE lub minimum 4 interfejsy sieciowe 10GbE
7	Wspierane systemy operacyjne: MS Windows 2008 R2, MS Windows 2012 R2, Red Hat Enterprise Linux ,SUSE Linux Enterprise Server, VMware 6.0.

9.2.2 Serwery RACK typ A – 8 szt.

Każdy z dostarczanych serwerów musi spełniać poniższe wymagania:

ID	Wymaganie
1	Zainstalowane 2 procesory, maksimum 6 rdzeni każdy, x86 - 64 Bit osiągające w testach SPECint_rate2006 wynik nie gorszy niż 700 punktów w konfiguracji dwuprocesorowej.
2	Zainstalowane 1TB RAM DDR4 Registred DIMMs lub LoadReduces DIMM w modułach min. 64GB.
3	2 dyski SSD typu Hot Swap, każdy o pojemności minimum 1TB.
4	Kontroler dysków obsługujący poziomy RAID 0/1.
5	2 redundantne zasilacze typu Hot-plug.
6	Zestaw redundantnych wentylatorów.
7	Minimum 2 sloty PCI-Express x16 (szybkość slotu).
8	Dwa Interfejsy SAN FC 16Gb.
9	Minimum 2 Interfejsy sieciowe 1GbE i 2 Interfejsy sieciowe 10GbE.
10	Wsperane systemy operacyjne: MS Windows 2008 R2, MS Windows 2012 R2, Red Hat Enterprise Linux.
11	Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS). Możliwość przejęcia zdalnej konsoli graficznej i podłączania wirtualnych napędów CD i FDD. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną. Wraz z serwerem należy dostarczyć oprogramowanie do zarządzania serwerem, pozwalające na: • Inwentaryzację sprzętu serwerowego, monitoring zdrowia - „health status” • zautomatyzowane instalacje systemu operacyjnego z wykorzystaniem mechanizmu PXE (bootowanie z sieci) • zautomatyzowane, personalizowane, zrównoleglone instalacje systemów operacyjnych oraz aplikacji z wykorzystaniem tzw. plików odpowiedzi dostarczanych przez producenta oprogramowania użytkowego • zautomatyzowane, zrównoleglone kopiowanie środowisk, połączone z natychmiastową personalizacją systemu • monitorowanie utylizacji następujących podzespołów serwera: procesor, pamięć i zasilania

9.2.3 Serwery RACK typ B - 6 szt.

Każdy z dostarczanych serwerów musi spełniać poniższe wymagania:

ID	Wymaganie
1	Zainstalowane 1 procesor, maksimum 6 rdzeni, x86 - 64 Bit osiągający w testach SPECint_rate2006 wynik nie gorszy niż 300 punktów.
2	Zainstalowane 512GB RAM DDR4 Registred DIMMs lub LoadReduces DIMM w modułach min. 64GB.
3	2 dyski SSD typu Hot Swap, każdy o pojemności minimum 1TB.
4	Kontroler dysków obsługujący poziomy RAID 0/1.
5	2 redundantne zasilacze typu Hot-plug.
6	Zestaw redundantnych wentylatorów.
7	Minimum 2 sloty PCI-Express x16 (szybkość slotu).
8	Dwa Interfejsy SAN FC 16Gb.
9	Minimum 2 Interfejsy sieciowe 1GbE i 2 Interfejsy sieciowe 10GbE.
10	Wsperane systemy operacyjne: MS Windows 2008 R2, MS Windows 2012 R2, Red Hat Enterprise Linux.
11	Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS). Możliwość przejęcia zdalnej konsoli graficznej i podłączania wirtualnych napędów CD i FDD. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną. Wraz z serwerem należy dostarczyć oprogramowanie do zarządzania serwerem, pozwalające na: • Inwentaryzację sprzętu serwerowego, monitoring zdrowia - „health status” • zautomatyzowane instalacje systemu operacyjnego z wykorzystaniem mechanizmu PXE (bootowanie z sieci) • zautomatyzowane, personalizowane, zrównoleglone instalacje systemów operacyjnych oraz aplikacji z wykorzystaniem tzw. plików odpowiedzi dostarczanych przez producenta oprogramowania użytkowego • zautomatyzowane, zrównoleglone kopiowanie środowisk, połączone z natychmiastową personalizacją systemu • monitorowanie utylizacji następujących podzespołów serwera: procesor, pamięć i zasilania

9.2.4 Konsola zarządzająca - 2 szt.

Produkt musi spełnić następujące wymagania:

ID	Wymaganie
1	Konsola składająca się z monitora (minimum 17’’), klawiatury i urządzenia wskazującego (track

	ball, touchpad, itp...). Zajmująca w szafie nie więcej niż 1U.
2	Zainstalowany wraz z konsolą przełącznik KVM zapewniający możliwość podłączenia minimum 8 oferowanych serwerów RACK, dostarczony komplet wymaganych adapterów/interfejsów. Całość rozwiązania ma zajmować w szafie 1U.

9.3 Macierze blokowe

9.3.1 Macierz blokowa typ A - 2szt.

Produkt musi spełnić następujące wymagania:

9.3.1.1 Wymagania ogólne

ID	Wymaganie
1	Oferowane urządzenie musi być dostarczone ze wszystkimi niezbędnymi komponentami do instalowania w szafie rack 19''.
2	Oferowane urządzenie musi posiadać kontrolery pracujące w trybie Active-Active z funkcją Mirrored cache.
3	Macierz musi być wyposażona w minimum 1024GB pamięci Cache obsługującej zapis i odczyt dostępnej dla wszystkich wolumenów macierzy (nie może to być funkcjonalność tieringu), musi być możliwość włączenia lub wyłączenia buforowania on-line (bez konieczności migracji bądź przenoszenia zawartości wolumenów).
4	Macierz musi posiadać system podtrzymania zawartości pamięci cache na wypadek awarii zasilania realizowany poprzez zapis danych z pamięci cache kontrolerów do pamięci typu flash lub równoważny zapewniający co najmniej taki sam czas przechowywania danych.
5	Macierz musi obsługiwać dyski 2,5” jak i 3,5”.
6	Macierz dyskowa musi umożliwiać stosowanie w niej dysków SSD, HDD 15k, HDD 10k i HDD 7,2k rpm wyposażonych w interfejsy SAS 12Gbps (SAS, NL-SAS).
7	Macierz musi być wyposażona w dyski posiadające podwójne interfejsy.
8	Macierz musi mieć możliwość instalacji dysków SSD, SAS, NL-SAS w tej samej półce dyskowej.
9	Oferowana macierz musi posiadać dla każdego kontrolera minimum 2 porty FC, obsadzone modułami światłowodowymi SFP+ 16 Gb/s
10	RAID w macierzy: obsługa poziomów RAID 1 lub 10, 5, 6.
11	Macierz musi obsługiwać protokół FC - jeśli wymagane są licencje Wykonawca dostarczy je wraz z macierzą.
12	Brak pojedynczego punktu awarii.

ID	Wymaganie
13	Redundantne zasilanie, chłodzenie, kontrolery, dwie ścieżki dostępu do każdego dysku.
14	Graficzny interfejs dostępny przez przeglądarkę oraz interfejs tekstowy przez szyfrowane połączenie.
15	Musi istnieć możliwość bezpośredniego monitoringu stanu w jakim w danym momencie macierz się znajduje.
16	Dane o parametrach wydajnościowych macierzy muszą być dostępne w postaci wykresów w interfejsie GUI.
17	Macierz musi posiadać funkcjonalność zarządzania całością dostępnych zasobów dyskowych, z jednej konsoli administracyjnej.
18	Wymagane jest aby dostarczona macierz posiadała interfejs zarządzający GUI, CLI, oraz umożliwiała tworzenie skryptów użytkownika.
19	Możliwość zarządzania całością dostępnych zasobów dyskowych z jednej konsoli administracyjnej. Zarządzanie w oparciu o użytkowników z przypisanymi uprawnieniami (role-based).
20	Musi istnieć możliwość bezpośredniego monitoringu stanu w jakim w danym momencie macierz się znajduje.
21	W pełni nadmiarowe wentylatory i zasilacze z możliwością wymiany podczas pracy.
22	Macierz musi umożliwiać wykonywanie aktualizacji mikrokodu macierzy w trybie online bez przerywania dostępu do zasobów dyskowych macierzy i przerywania pracy aplikacji.
23	Macierz musi zapewniać funkcjonalność udostępniania przestrzeni bez konieczności fizycznego alokowania wolnego miejsca na dyskach (thin provisioning). Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla całej macierzy w maksymalnej konfiguracji.
24	Macierz musi umożliwiać zwrot zwolnionej przestrzeni dyskowej do puli.
25	Macierz musi posiadać funkcjonalność tieringu polegającą na automatycznej migracji bloków danych dysków logicznych pomiędzy różnymi typami dysków fizycznych (SSD, SAS/FC, NLSAS/SATA), w zależności od stopnia wykorzystania danego obszaru przez aplikację. Migracje muszą być wykonywane automatycznie bez udziału administratora. Migracja danych musi odbywać się bez przerywania dostępu do danych od strony hostów i aplikacji.
26	Macierz musi umożliwiać automatyczne rozkładanie bloków dysków logicznych pomiędzy wszystkie dostępne dyski fizyczne funkcjonujące w ramach tej samej puli/grupy dyskowej w przypadku rozszerzania dysku logicznego i dokładania dysków fizycznych.
27	Macierz musi obsługiwać LUN Masking i Lun mapping.
28	Sterowniki do obsługi wielościeżkowego dostępu do wolumenów, awarii ścieżki i rozłożenia obciążenia po ścieżkach dostępu mają być dostępne dla podłączanych systemów operacyjnych. Jeżeli zastosowanie tych sterowników wymaga licencji, musi być dostarczona dla podłączanych

ID	Wymaganie
	systemów operacyjnych
29	Macierz musi posiadać funkcjonalność zwiększania rozmiaru wolumenów.
30	Macierz powinna zapewniać wykonywanie kopii migawkowych w ilości minimum 256 dla wolumenu logicznego. Przepełnienie przestrzeni dla kopii migawkowych nie może powodować błędów zapisu na przestrzeń produkcyjną. Licencja umożliwiająca wykorzystanie powyższej funkcjonalności jest obecnie przedmiotem zamówienia.
31	Macierz musi wspierać mechanizm zdalnej replikacji w trybie synchronicznym i asynchronicznym. Licencja umożliwiająca wykorzystanie powyższej funkcjonalności jest przedmiotem zamówienia.
32	Obsługiwane systemy operacyjne: Microsoft Windows 2008/2008R2/2012/2012R2, Suse 11/12, Redhat 5/6/7, Solaris 11, VMware 5.0/5.1/5.5/6.0, vVOL.
33	Wymagane jest dostarczenie macierzy dyskowej spełniającej wymagania pojemnościowe: Macierz dyskowa składająca się z 3 obszarów dyskowych: I - zapewniającego bardzo wysoką wydajność - musi zawierać dyski SSD udostępniając użytkownikowi powierzchnię użytkową (dla której nie wliczają się dyski parzystości i dyski hot spare) minimum 27TB w konfiguracji RAID 5** II - zapewniającego wysoką wydajność - musi zawierać dyski SAS o prędkości obrotowej nie mniejszej niż 10k RPM w ilości minimum 90 sztuk udostępniając użytkownikowi powierzchnię użytkową (dla której nie wliczają się dyski parzystości i dyski hot spare) minimum 128TB w konfiguracji RAID 5** III - zapewniającego wysoką pojemność - musi zawierać dyski SAS/NL-SAS o prędkości obrotowej nie mniejszej niż 7,2k RPM w ilości minimum 40 sztuk udostępniając użytkownikowi powierzchnię użytkową (dla której nie wliczają się dyski parzystości i dyski hot spare) minimum 161TB w konfiguracji RAID 6** Należy wyposażyć macierz w niezbędne dyski zapasowe (spare) zgodnie z zaleceniami producenta macierzy (nie mniej niż 1 sztuka na 30 dysków). Wszystkie dyski oferowanej i dostarczonej macierzy muszą pracować w trybie „Hot-Plug". W każdym z obszarów wszystkie dyski muszą być tego samego typu i pojemności Nie dopuszcza się stosowania dysków cMLC a jedynie dyski klasy eMLC. ** - Należy przyjąć, że 1 TB=1024GB, 1 GB=1024MB, 1MB=1024kB, 1kB=1024B i grupy dyskowe RAID nie większe niż 9 dysków dla RAID 5 oraz 8 dysków dla RAID 6.
34	Oferowana macierz ma nie mniej niż 1024GB pamięci cache.

9.3.1.2 Wymagania na moduł wirtualizacji zasobów dyskowych na poziomie sieci SAN.

	Macierze należy wyposażyć w moduł wirtualizacji zasobów dyskowych na poziomie sieci SAN o poniższych wymaganiach

	Macierze należy wyposażyć w moduł wirtualizacji zasobów dyskowych na poziomie sieci SAN o poniższych wymaganiach
35	Oferowane rozwiązanie musi umożliwiać wirtualizację zasobów dyskowych macierzy dyskowych pochodzących od różnych dostawców, m. in. HP, IBM, EMC, HDS. Wymagane jest dostarczenie licencji na maksymalną pojemność oferowanych macierzy.
36	Oferowane rozwiązanie musi umożliwiać prezentacje zwirtualizowanych zasobów dyskowych do aplikacji pracujących na różnych platformach OS, mi. In: IBM AIX, HP-UX, Linux, MS Windows, Solaris, VMware.
37	Oferowane rozwiązanie musi umożliwiać prezentowanie do aplikacji wolumenów logicznych wystawionych z macierzy dyskowych w sposób nienaruszający zawartości tych wolumenów (prezentacja 1 do 1). Oferowane rozwiązanie musi umożliwiać połączenie macierzy w dwóch oddalonych od siebie centrach przetwarzania danych (ośrodkach) w celu umożliwienia wirtualizacji zasobów dyskowych pomiędzy tymi centrami – rozwiązanie separowane geograficznie.
38	Wymagane jest, aby oferowane rozwiązanie umożliwiało transmisję danych pomiędzy ośrodkami w trybie synchronicznym. Wymagane jest, aby rozwiązanie separowane geograficznie umożliwiało oddalenie pary wirtualizatorów na odległość, dla której opóźnienie transmisji danych RTT dochodzi do 5ms.
39	Wirtualny wolumen logiczny prezentowany w obu lokalizacjach, zbudowany jest w oparciu o parę fizycznych wolumenów logicznych połączonych ze sobą zdalną replikacją danych (kopia lustrzana realizowana pomiędzy lokalizacjami). Wymagane jest zapewnienie spójności danych dla synchronicznego trybu replikacji. Wymagana jest możliwość zbudowania klastra rozległego oraz przełączenia przetwarzania pomiędzy lokalizacjami bez jakiejkolwiek przerwy w dostępie do danych. Wymagana jest możliwość zbudowania klastra rozległego oraz przełączenia przetwarzania pomiędzy lokalizacjami bez jakiejkolwiek przerwy w dostępie do danych w szczególności dla: Oracle Real Application Cluster, VMware HA oraz MS Cluster.
40	Wymagane jest, aby rozwiązanie separowane geograficznie umożliwiało zastosowanie arbitra, znajdującego się w trzeciej lokalizacji, w celu uniknięcia zjawiska split-brain w przypadku awarii komunikacji pomiędzy centrami przetwarzania danych.
41	Oferowane rozwiązanie separowane geograficznie musi posiadać mechanizmy umożliwiające pracę, przy zachowaniu pełnej funkcjonalności oraz bezpieczeństwa i spójności danych także bez stosowania arbitra.
42	Oferowane rozwiązanie wirtualizujące musi posiadać wsparcie dla protokołów VAAI (CompareAndWrite SCSI Command) oraz VASA.
43	Oferowane rozwiązanie musi być odporne na awarię pojedynczego elementu.
44	Oferowane rozwiązanie musi umożliwiać naprawę, rozbudowę, aktualizacje oprogramowania wewnętrznego w sposób nieprzerywający dostępu do danych. Awaria dowolnego pojedynczego kontrolera rozwiązania nie może wymuszać konieczności przełączenia pracy aplikacji do drugiego ośrodka lub ręcznej rekonfiguracji środowiska.

	Macierze należy wyposażyć w moduł wirtualizacji zasobów dyskowych na poziomie sieci SAN o poniższych wymaganiach
45	W celu zapewnienia dostępności oraz wydajności oferowane rozwiązanie musi umożliwiać prezentowanie każdego wirtualnego wolumenu logicznego do serwerów poprzez wszystkie kontrolery oferowanego rozwiązania jednocześnie, także po rozbudowie do maksymalnej liczby kontrolerów
46	Oferowane rozwiązanie wirtualizacyjne (dla pojedynczej lokalizacji) ma być wyposażone w co najmniej: • 2 kontrolery z możliwością rozbudowy do co najmniej 4, • 10 portów FC 16 Gb/s na kontroler, • 128 GB pamięci podręcznej brutto na kontroler.
47	Dla rozwiązania wirtualizacyjnego wsparcie dla operacji vMotion dla parametrów łącza pomiędzy site RTT=10ms

9.3.2 Macierz blokowa typ B – 1 szt.

Produkt musi spełnić następujące wymagania:

9.3.2.1 Wymagania ogólne

ID	Wymaganie
1	Oferowane urządzenie musi być dostarczone ze wszystkimi niezbędnymi komponentami do instalowania w szafie rack 19''.
2	Oferowane urządzenie musi posiadać kontrolery pracujące w trybie Active-Active z funkcją Mirrored cache.
3	Macierz musi być wyposażona w minimum 1024GB pamięci Cache obsługującej zapis i odczyt dostępnej dla wszystkich wolumenów macierzy (nie może to być funkcjonalność tieringu), musi być możliwość włączenia lub wyłączenia buforowania on-line (bez konieczności migracji bądź przenoszenia zawartości wolumenów).
4	Macierz musi posiadać system podtrzymania zawartości pamięci cache na wypadek awarii zasilania realizowany poprzez zapis danych z pamięci cache kontrolerów do pamięci typu flash lub równoważny zapewniający co najmniej taki sam czas przechowywania danych.
5	Macierz musi obsługiwać dyski 2,5” jak i 3,5”.
6	Macierz dyskowa musi umożliwiać stosowanie w niej dysków SSD, HDD 15k, HDD 10k i HDD 7,2k rpm wyposażonych w interfejsy SAS 12Gbps (SAS, NL-SAS).
7	Macierz musi być wyposażona w dyski posiadające podwójne interfejsy.
8	Macierz musi mieć możliwość instalacji dysków SSD, SAS, NL-SAS w tej samej półce dyskowej.
9	Oferowana macierz musi posiadać dla każdego kontrolera minimum 2 porty FC, obsadzone modułami światłowodowymi SFP+ 16 Gb/s

ID	Wymaganie
10	RAID w macierzy: obsługa poziomów RAID 1 lub 10, 5, 6.
11	Macierz musi obsługiwać protokół FC - jeśli wymagane są licencje Wykonawca dostarczy je wraz z macierzą.
12	Brak pojedynczego punktu awarii.
13	Redundantne zasilanie, chłodzenie, kontrolery, dwie ścieżki dostępu do każdego dysku.
14	Graficzny interfejs dostępny przez przeglądarkę oraz interfejs tekstowy przez szyfrowane połączenie.
15	Musi istnieć możliwość bezpośredniego monitoringu stanu w jakim w danym momencie macierz się znajduje.
16	Dane o parametrach wydajnościowych macierzy muszą być dostępne w postaci wykresów w interfejsie GUI.
17	Macierz musi posiadać funkcjonalność zarządzania całością dostępnych zasobów dyskowych, z jednej konsoli administracyjnej.
18	Wymagane jest aby dostarczona macierz posiadała interfejs zarządzający GUI, CLI, oraz umożliwiała tworzenie skryptów użytkownika.
19	Możliwość zarządzania całością dostępnych zasobów dyskowych z jednej konsoli administracyjnej. Zarządzanie w oparciu o użytkowników z przypisanymi uprawnieniami (role-based).
20	Musi istnieć możliwość bezpośredniego monitoringu stanu w jakim w danym momencie macierz się znajduje.
21	W pełni nadmiarowe wentylatory i zasilacze z możliwością wymiany podczas pracy.
22	Macierz musi umożliwiać wykonywanie aktualizacji mikrokodu macierzy w trybie online bez przerywania dostępu do zasobów dyskowych macierzy i przerywania pracy aplikacji.
23	Macierz musi zapewniać funkcjonalność udostępniania przestrzeni bez konieczności fizycznego alokowania wolnego miejsca na dyskach (thin provisioning). Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla całej macierzy w maksymalnej konfiguracji.
24	Macierz musi umożliwiać zwrot zwolnionej przestrzeni dyskowej do puli.
25	Macierz musi posiadać funkcjonalność tieringu polegającą na automatycznej migracji bloków danych dysków logicznych pomiędzy różnymi typami dysków fizycznych (SSD, SAS/FC, NLSAS/SATA), w zależności od stopnia wykorzystania danego obszaru przez aplikację. Migracje muszą być wykonywane automatycznie bez udziału administratora. Migracja danych musi odbywać się bez przerywania dostępu do danych od strony hostów i aplikacji.
26	Macierz musi umożliwiać automatyczne rozkładanie bloków dysków logicznych pomiędzy wszystkie dostępne dyski fizyczne funkcjonujące w ramach tej samej puli/grupy dyskowej

ID	Wymaganie
	w przypadku rozszerzania dysku logicznego i dokładania dysków fizycznych.
27	Macierz musi obsługiwać LUN Masking i Lun mapping.
28	Sterowniki do obsługi wielościeżkowego dostępu do wolumenów, awarii ścieżki i rozłożenia obciążenia po ścieżkach dostępu mają być dostępne dla podłączanych systemów operacyjnych. Jeżeli zastosowanie tych sterowników wymaga licencji, musi być dostarczona dla podłączanych systemów operacyjnych
29	Macierz musi posiadać funkcjonalność zwiększania rozmiaru wolumenów.
30	Macierz powinna zapewniać wykonywanie kopii migawkowych w ilości minimum 256 dla wolumenu logicznego. Przepełnienie przestrzeni dla kopii migawkowych nie może powodować błędów zapisu na przestrzeń produkcyjną. Licencja umożliwiająca wykorzystanie powyższej funkcjonalności jest obecnie przedmiotem zamówienia.
31	Macierz musi wspierać mechanizm zdalnej replikacji w trybie synchronicznym i asynchronicznym. Licencja umożliwiająca wykorzystanie powyższej funkcjonalności jest przedmiotem zamówienia.
32	Obsługiwane systemy operacyjne: Microsoft Windows 2008/2008R2/2012/2012R2, Suse 11/12, Redhat 5/6/7, Solaris 11, VMware 5.0/5.1/5.5/6.0, vVOL.
33	Wymagane jest dostarczenie macierzy dyskowej spełniającej wymagania pojemnościowe: Macierz dyskowa składająca się z 2 obszarów dyskowych: I - zapewniającego bardzo wysoką wydajność - musi zawierać dyski SSD w ilości minimum 38 sztuk udostępniając użytkownikowi powierzchnię użytkową (dla której nie wliczają się dyski parzystości i dyski hot spare) minimum 91TB w konfiguracji RAID 5** II - zapewniającego wysoką wydajność - musi zawierać dyski SAS o prędkości obrotowej nie mniejszej niż 10k RPM w ilości minimum 121 sztuk udostępniając użytkownikowi powierzchnię użytkową (dla której nie wliczają się dyski parzystości i dyski hot spare) minimum 111TB w konfiguracji RAID 5** Należy wyposażyć macierz w niezbędne dyski zapasowe (spare) zgodnie z zaleceniami producenta macierzy (nie mniej niż 1 sztuka na 30 dysków). Wszystkie dyski oferowanej i dostarczonej macierzy muszą pracować w trybie „Hot-Plug". W każdym z obszarów wszystkie dyski muszą być tego samego typu i pojemności Nie dopuszcza się stosowania dysków cMLC a jedynie dyski klasy eMLC. ** - Należy przyjąć, że 1 TB=1024GB, 1 GB=1024MB, 1MB=1024kB, 1kB=1024B i grupy dyskowe RAID nie większe niż 9 dysków dla RAID 5.
34	Oferowana macierz ma nie mniej niż 1024GB pamięci cache.

9.3.2.2 Wymagania na moduł wirtualizacji zasobów dyskowych na poziomie sieci SAN.

	Macierz należy wyposażyć w moduł wirtualizacji zasobów dyskowych na poziomie sieci SAN o poniższych wymaganiach

35	Oferowane rozwiązanie musi umożliwiać wirtualizację zasobów dyskowych macierzy dyskowych pochodzących od różnych dostawców, m. in. HP, IBM, EMC, HDS. Wymagane jest dostarczenie licencji na maksymalną pojemność oferowanych macierzy.
36	Oferowane rozwiązanie musi umożliwiać prezentacje zwirtualizowanych zasobów dyskowych do aplikacji pracujących na różnych platformach OS, mi. In: IBM AIX, HP-UX, Linux, MS Windows, Solaris, VMware.
37	Oferowane rozwiązanie musi umożliwiać prezentowanie do aplikacji wolumenów logicznych wystawionych z macierzy dyskowych w sposób nienaruszający zawartości tych wolumenów (prezentacja 1 do 1). Oferowane rozwiązanie musi umożliwiać połączenie macierzy w dwóch oddalonych od siebie centrach przetwarzania danych (ośrodkach) w celu umożliwienia wirtualizacji zasobów dyskowych pomiędzy tymi centrami – rozwiązanie separowane geograficznie.
38	Wymagane jest, aby oferowane rozwiązanie umożliwiało transmisję danych pomiędzy ośrodkami w trybie synchronicznym. Wymagane jest, aby rozwiązanie separowane geograficznie umożliwiało oddalenie pary wirtualizatorów na odległość, dla której opóźnienie transmisji danych RTT dochodzi do 5ms.
39	Wirtualny wolumen logiczny prezentowany w obu lokalizacjach, zbudowany jest w oparciu o parę fizycznych wolumenów logicznych połączonych ze sobą zdalną replikacją danych (kopia lustrzana realizowana pomiędzy lokalizacjami). Wymagane jest zapewnienie spójności danych dla synchronicznego trybu replikacji. Wymagana jest możliwość zbudowania klastra rozległego oraz przełączenia przetwarzania pomiędzy lokalizacjami bez jakiejkolwiek przerwy w dostępie do danych. Wymagana jest możliwość zbudowania klastra rozległego oraz przełączenia przetwarzania pomiędzy lokalizacjami bez jakiejkolwiek przerwy w dostępie do danych w szczególności dla: Oracle Real Application Cluster, VMware HA oraz MS Cluster.
40	Wymagane jest, aby rozwiązanie separowane geograficznie umożliwiało zastosowanie arbitra, znajdującego się w trzeciej lokalizacji, w celu uniknięcia zjawiska split-brain w przypadku awarii komunikacji pomiędzy centrami przetwarzania danych.
41	Oferowane rozwiązanie separowane geograficznie musi posiadać mechanizmy umożliwiające pracę, przy zachowaniu pełnej funkcjonalności oraz bezpieczeństwa i spójności danych także bez stosowania arbitra.
42	Oferowane rozwiązanie wirtualizujące musi posiadać wsparcie dla protokołów VAAI (CompareAndWrite SCSI Command) oraz VASA.
43	Oferowane rozwiązanie musi być odporne na awarię pojedynczego elementu.
44	Oferowane rozwiązanie musi umożliwiać naprawę, rozbudowę, aktualizacje oprogramowania wewnętrznego w sposób nieprzerywający dostępu do danych. Awaria dowolnego pojedynczego kontrolera rozwiązania nie może wymuszać konieczności przełączenia pracy aplikacji do drugiego ośrodka lub ręcznej rekonfiguracji środowiska.
45	W celu zapewnienia dostępności oraz wydajności oferowane rozwiązanie musi umożliwiać prezentowanie każdego wirtualnego wolumenu logicznego do serwerów poprzez wszystkie kontrolery oferowanego rozwiązania jednocześnie, także po rozbudowie do maksymalnej liczby kontrolerów

46	Oferowane rozwiązanie wirtualizacyjne (dla pojedynczej lokalizacji) ma być wyposażone w co najmniej: • 2 kontrolery z możliwością rozbudowy do co najmniej 4, • 10 portów FC 16 Gb/s na kontroler, • 128 GB pamięci podręcznej brutto na kontroler.
47	Dla rozwiązania wirtualizacyjnego wsparcie dla operacji vMotion dla parametrów łącza pomiędzy site RTT=10ms

9.3.3 Macierz blokowa typ C – 1 szt.

Produkt musi spełnić następujące wymagania:

9.3.3.1 Wymagania ogólne

ID	Wymaganie
1	Oferowane urządzenie musi być dostarczone ze wszystkimi niezbędnymi komponentami do instalowania w szafie rack 19''.
2	Oferowane urządzenie musi posiadać kontrolery pracujące w trybie Active-Active z funkcją Mirrored cache.
3	Macierz musi być wyposażona w minimum 1024GB pamięci Cache obsługującej zapis i odczyt dostępnej dla wszystkich wolumenów macierzy (nie może to być funkcjonalność tieringu), musi być możliwość włączenia lub wyłączenia buforowania on-line (bez konieczności migracji bądź przenoszenia zawartości wolumenów).
4	Macierz musi posiadać system podtrzymania zawartości pamięci cache na wypadek awarii zasilania realizowany poprzez zapis danych z pamięci cache kontrolerów do pamięci typu flash lub równoważny zapewniający co najmniej taki sam czas przechowywania danych.
5	Macierz musi obsługiwać dyski 2,5” jak i 3,5”.
6	Macierz dyskowa musi umożliwiać stosowanie w niej dysków SSD, HDD 15k, HDD 10k i HDD 7,2k rpm wyposażonych w interfejsy SAS 12Gbps (SAS, NL-SAS).
7	Macierz musi być wyposażona w dyski posiadające podwójne interfejsy.
8	Macierz musi mieć możliwość instalacji dysków SSD, SAS, NL-SAS w tej samej półce dyskowej.
9	Oferowana macierz musi posiadać dla każdego kontrolera minimum 2 porty FC, obsadzone modułami światłowodowymi SFP+ 16 Gb/s
10	RAID w macierzy: obsługa poziomów RAID 1 lub 10, 5, 6.
11	Macierz musi obsługiwać protokół FC - jeśli wymagane są licencje Wykonawca dostarczy je wraz z macierzą.
12	Brak pojedynczego punktu awarii.

ID	Wymaganie
13	Redundantne zasilanie, chłodzenie, kontrolery, dwie ścieżki dostępu do każdego dysku.
14	Graficzny interfejs dostępny przez przeglądarkę oraz interfejs tekstowy przez szyfrowane połączenie.
15	Musi istnieć możliwość bezpośredniego monitoringu stanu w jakim w danym momencie macierz się znajduje.
16	Dane o parametrach wydajnościowych macierzy muszą być dostępne w postaci wykresów w interfejsie GUI.
17	Macierz musi posiadać funkcjonalność zarządzania całością dostępnych zasobów dyskowych, z jednej konsoli administracyjnej.
18	Wymagane jest aby dostarczona macierz posiadała interfejs zarządzający GUI, CLI, oraz umożliwiała tworzenie skryptów użytkownika.
19	Możliwość zarządzania całością dostępnych zasobów dyskowych z jednej konsoli administracyjnej. Zarządzanie w oparciu o użytkowników z przypisanymi uprawnieniami (role-based).
20	Musi istnieć możliwość bezpośredniego monitoringu stanu w jakim w danym momencie macierz się znajduje.
21	W pełni nadmiarowe wentylatory i zasilacze z możliwością wymiany podczas pracy.
22	Macierz musi umożliwiać wykonywanie aktualizacji mikrokodu macierzy w trybie online bez przerywania dostępu do zasobów dyskowych macierzy i przerywania pracy aplikacji.
23	Macierz musi zapewniać funkcjonalność udostępniania przestrzeni bez konieczności fizycznego alokowania wolnego miejsca na dyskach (thin provisioning). Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla całej macierzy w maksymalnej konfiguracji.
24	Macierz musi umożliwiać zwrot zwolnionej przestrzeni dyskowej do puli.
25	Macierz musi posiadać funkcjonalność tieringu polegającą na automatycznej migracji bloków danych dysków logicznych pomiędzy różnymi typami dysków fizycznych (SSD, SAS/FC, NLSAS/SATA), w zależności od stopnia wykorzystania danego obszaru przez aplikację. Migracje muszą być wykonywane automatycznie bez udziału administratora. Migracja danych musi odbywać się bez przerywania dostępu do danych od strony hostów i aplikacji.
26	Macierz musi umożliwiać automatyczne rozkładanie bloków dysków logicznych pomiędzy wszystkie dostępne dyski fizyczne funkcjonujące w ramach tej samej puli/grupy dyskowej w przypadku rozszerzania dysku logicznego i dokładania dysków fizycznych.
27	Macierz musi obsługiwać LUN Masking i Lun mapping.
28	Sterowniki do obsługi wielościeżkowego dostępu do wolumenów, awarii ścieżki i rozłożenia obciążenia po ścieżkach dostępu mają być dostępne dla podłączanych systemów operacyjnych. Jeżeli zastosowanie tych sterowników wymaga licencji, musi być dostarczona dla podłączanych

ID	Wymaganie
	systemów operacyjnych
29	Macierz musi posiadać funkcjonalność zwiększania rozmiaru wolumenów.
30	Macierz powinna zapewniać wykonywanie kopii migawkowych w ilości minimum 256 dla wolumenu logicznego. Przepełnienie przestrzeni dla kopii migawkowych nie może powodować błędów zapisu na przestrzeń produkcyjną. Licencja umożliwiająca wykorzystanie powyższej funkcjonalności jest obecnie przedmiotem zamówienia.
31	Macierz musi wspierać mechanizm zdalnej replikacji w trybie synchronicznym i asynchronicznym. Licencja umożliwiająca wykorzystanie powyższej funkcjonalności jest przedmiotem zamówienia.
32	Obsługiwane systemy operacyjne: Microsoft Windows 2008/2008R2/2012/2012R2, Suse 11/12, Redhat 5/6/7, Solaris 11, VMware 5.0/5.1/5.5/6.0, vVOL.
33	Wymagane jest dostarczenie macierzy dyskowej spełniającej wymagania pojemnościowe: Macierz dyskowa składająca się z 1 obszaru dyskowego: I - zapewniającego wysoką wydajność - musi zawierać dyski SAS o prędkości obrotowej nie mniejszej niż 10k RPM w ilości minimum 224 sztuk udostępniając użytkownikowi powierzchnię użytkową (dla której nie wliczają się dyski parzystości i dyski hot spare) minimum 206TB w konfiguracji RAID 5** Należy wyposażyć macierz w niezbędne dyski zapasowe (spare) zgodnie z zaleceniami producenta macierzy (nie mniej niż 1 sztuka na 30 dysków). Wszystkie dyski oferowanej i dostarczonej macierzy muszą pracować w trybie „Hot-Plug”. W każdym z obszarów wszystkie dyski muszą być tego samego typu i pojemności ** - Należy przyjąć, że 1 TB=1024GB, 1 GB=1024MB, 1MB=1024kB, 1kB=1024B i grupy dyskowe RAID nie większe niż 9 dysków dla RAID 5.
34	Oferowana macierz ma nie mniej niż 1024GB pamięci cache.

9.3.3.2 Wymagania na moduł wirtualizacji zasobów dyskowych na poziomie sieci SAN.

	Macierz należy wyposażyć w moduł wirtualizacji zasobów dyskowych na poziomie sieci SAN. O poniższych wymaganiach
35	Oferowane rozwiązanie musi umożliwiać wirtualizację zasobów dyskowych macierzy dyskowych pochodzących od różnych dostawców, m. in. HP, IBM, EMC, HDS. Wymagane jest dostarczenie licencji na maksymalną pojemność oferowanych macierzy.
36	Oferowane rozwiązanie musi umożliwiać prezentacje zwirtualizowanych zasobów dyskowych do aplikacji pracujących na różnych platformach OS, mi. In: IBM AIX, HP-UX, Linux, MS Windows, Solaris, VMware.

37	Oferowane rozwiązanie musi umożliwiać prezentowanie do aplikacji wolumenów logicznych wystawionych z macierzy dyskowych w sposób nienaruszający zawartości tych wolumenów (prezentacja 1 do 1). Oferowane rozwiązanie musi umożliwiać połączenie macierzy w dwóch oddalonych od siebie centrach przetwarzania danych (ośrodkach) w celu umożliwienia wirtualizacji zasobów dyskowych pomiędzy tymi centrami – rozwiązanie separowane geograficznie.
38	Wymagane jest, aby oferowane rozwiązanie umożliwiało transmisję danych pomiędzy ośrodkami w trybie synchronicznym. Wymagane jest, aby rozwiązanie separowane geograficznie umożliwiało oddalenie pary wirtualizatorów na odległość, dla której opóźnienie transmisji danych RTT dochodzi do 5ms.
39	Wirtualny wolumen logiczny prezentowany w obu lokalizacjach, zbudowany jest w oparciu o parę fizycznych wolumenów logicznych połączonych ze sobą zdalną replikacją danych (kopia lustrzana realizowana pomiędzy lokalizacjami). Wymagane jest zapewnienie spójności danych dla synchronicznego trybu replikacji. Wymagana jest możliwość zbudowania klastra rozległego oraz przełączenia przetwarzania pomiędzy lokalizacjami bez jakiejkolwiek przerwy w dostępie do danych. Wymagana jest możliwość zbudowania klastra rozległego oraz przełączenia przetwarzania pomiędzy lokalizacjami bez jakiejkolwiek przerwy w dostępie do danych w szczególności dla: Oracle Real Application Cluster, VMware HA oraz MS Cluster.
40	Wymagane jest, aby rozwiązanie separowane geograficznie umożliwiało zastosowanie arbitra, znajdującego się w trzeciej lokalizacji, w celu uniknięcia zjawiska split-brain w przypadku awarii komunikacji pomiędzy centrami przetwarzania danych.
41	Oferowane rozwiązanie separowane geograficznie musi posiadać mechanizmy umożliwiające pracę, przy zachowaniu pełnej funkcjonalności oraz bezpieczeństwa i spójności danych także bez stosowania arbitra.
42	Oferowane rozwiązanie wirtualizujące musi posiadać wsparcie dla protokołów VAAI (CompareAndWrite SCSI Command) oraz VASA.
43	Oferowane rozwiązanie musi być odporne na awarię pojedynczego elementu.
44	Oferowane rozwiązanie musi umożliwiać naprawę, rozbudowę, aktualizacje oprogramowania wewnętrznego w sposób nieprzerywający dostępu do danych. Awaria dowolnego pojedynczego kontrolera rozwiązania nie może wymuszać konieczności przełączenia pracy aplikacji do drugiego ośrodka lub ręcznej rekonfiguracji środowiska.
45	W celu zapewnienia dostępności oraz wydajności oferowane rozwiązanie musi umożliwiać prezentowanie każdego wirtualnego wolumenu logicznego do serwerów poprzez wszystkie kontrolery oferowanego rozwiązania jednocześnie, także po rozbudowie do maksymalnej liczby kontrolerów
46	Oferowane rozwiązanie wirtualizacyjne (dla pojedynczej lokalizacji) ma być wyposażone w co najmniej: • 2 kontrolery z możliwością rozbudowy do co najmniej 4, • 10 portów FC 16 Gb/s na kontroler, • 128 GB pamięci podręcznej brutto na kontroler.
47	Dla rozwiązania wirtualizacyjnego wsparcie dla operacji vMotion dla parametrów łącza

	pomiędzy site RTT=10ms

9.4 Rozwiązanie NAS

Rozwiązanie NAS typ A ma pracować jako główne rozwiązanie. Dane z rozwiązania NAS typ A mają być replikowane synchronicznie lub asynchronicznie do rozwiązania NAS typ B. Dane z rozwiązania NAS typ B mają być replikowane asynchronicznie do rozwiązania NAS typ C i zapewnić kopie przyrostowe danych, tzn. zmiany danych w rozwiązaniu NAS typ B nie powinny nadpisywać wcześniej zreplikowanych danych w rozwiązania NAS typ C.

9.4.1 Rozwiązanie NAS typ A - 1szt.

Produkt musi spełnić następujące wymagania:

9.4.1.1 Wymagania ogólne

ID	Wymaganie
1	Pojemność użyteczna oferowanego rozwiązania pamięci dyskowej na dane użytkowników musi wynosić nie mniej niż 2000TiB w obrębie jednego systemu plików przy zachowaniu dostępu do danych w przypadku awarii, co najmniej trzech dowolnych półek jednocześnie, albo trzech dowolnych dysków.
2	Pojemność ma być zbudowana na dyskach NLSAS nie większych niż 4TB oraz dyskach SSD nie mniejszych niż 1.6TB.
3	Co najmniej 19 kontrolerów gdzie każdy realizuje dostęp plikowy do danych.
4	Rozwiązanie musi umożliwiać rozbudowę, do co najmniej 24 kontrolerów w ramach tego samego systemu dyskowego.
5	Dla maksymalizacji gęstości, tj. minimalizacji wykorzystania obszaru serwerowni do przechowywania danych, półka dyskowa lub węzeł stanowiący element rozwiązania pamięci dyskowej musi mieścić nie mniej, niż 6 dysków typu NL-SAS lub SAS w przeliczeniu na 1U (tj. np. nie mniej, niż 24 dyski w obudowie 4U).
6	Rozwiązanie pamięci dyskowej musi udostępniać całkowitą dostępną przestrzeń w ramach jednego ciągłego systemu plików.
7	Rozwiązanie pamięci dyskowej musi zapewniać dostępną, łączną pojemność pamięci cache typu RAM nie mniejszą niż 1200 GB. Ze względu na przewidywane obciążenie i wymaganą wydajność nie dopuszcza się realizacji pamięci w oparciu o dyski SSD.
8	Oferowane rozwiązanie musi zawierać nie mniej niż 19 dysków SSD o pojemności nie mniejszej niż 1.6TB każdy. Dyski SSD muszą być wykorzystywane do zwiększenia wydajności całości rozwiązania.
9	Rozwiązanie musi umożliwiać zwiększenie trzykrotne pojemności bez wprowadzania zmian do zaproponowanych kontrolerów.

10	Oferowane urządzenie musi umożliwiać dynamiczne rozszerzanie pojemności systemu plików w oparciu o całą pojemność fizyczną dodawaną do klastra bez konieczności: - modyfikacji już zainstalowanych kontrolerów, - restartu systemu, - ręcznej migracji/dystrybucji danych na nowe dyski systemu.
11	System plików zawarty w oferowanym rozwiązaniu musi być skalowalny, do co najmniej 10 PiB powierzchni netto.
12	System musi obsługiwać następujące protokoły plikowe: NFS V3 i V4, CIFS 2.0 i 3.0, FTP.
13	System musi zapewniać dostęp z różnych systemów operacyjnych (UNIX, Mac, Linux, Windows) z wykorzystaniem wszystkich standardowych protokołów: NFS, SMB (CIFS), HTTP, FTP. Wszystkie protokoły muszą być włączone bez dodatkowych licencji i sprzętu.
14	Rozwiązanie musi zapewniać wsparcie dla SMB multi-channel pozwalając na korzystanie z kilku kanałów komunikacji dla zwiększenia przepustowości, tolerancje awarii jednego z połączeń I automatycznego wychwycenia tego typu awarii.
15	Oferowane rozwiązanie pamięci dyskowej musi obsługiwać protokół NDMP w wersji 4 dla kopii zapasowych na taśmach, z dowolnego obszaru systemu plików.
16	Oferowane rozwiązanie pamięci dyskowej musi zapewnić gwarantowaną ochronę przed „cichym uszkodzeniem dysków” (silent data corruption) dla wszystkich technologii dyskowych (w tym SATA).
17	Oferowane rozwiązanie pamięci dyskowej musi umożliwiać wymianę uszkodzonego dysku przy zachowaniu nieprzerwanej dostępności wszystkich zasobów, tj. bez czasowego wyłączania z użycia innych elementów urządzenia. Musi istnieć możliwość jasnego określenia lokalizacji uszkodzonego dysku, np. za pomocą lampki kontrolnej lub wyświetlenia numeru pojedynczej zatoki/kieszeni.
18	Rozwiązanie pamięci dyskowej musi zapewniać pracę jednocześnie wszystkich kontrolerów w trybie aktywny/aktywny dla zapewnienia niezawodności i dostępności danych.
19	W przypadku awarii jednego dysku, czas od momentu jego wymiany do odzyskania pierwotnego poziomu ochrony danych nie może być dłuższy niż 12 godzin – w sytuacji braku obciążenia przez urządzenia klienckie.
20	Użytkownicy sieci muszą uzyskiwać dostęp do systemu pamięci masowej przy wykorzystaniu wewnętrznego load balancingu bez konieczności stosowania zewnętrznych urządzeń równoważących obciążenie. Powyższe wymaganie nie dotyczy rozwiązań opartych na dwóch kontrolerach.
21	Rozwiązanie pamięci masowej musi posiadać mechanizm równoważenia nowych połączeń pomiędzy kontrolerami zgodnie z polityką wyboru kontrolera: kontroler o najmniejszej liczbie połączeń, kontroler o najmniejszym wykorzystaniu CPU, polityka roundrobin. Powyższe wymaganie nie dotyczy rozwiązań opartych na dwóch kontrolerach.
22	Rozwiązanie pamięci dyskowej musi posiadać funkcjonalność replikacji synchronicznej lub asynchronicznej danych.

23	Każde z rozwiązań pamięci masowej musi realizować replikację asynchroniczną danych na poziomie pojedynczego katalogu celem dystrybucji treści i zapewnienia kopii danych z oferowanym "rozwiązaniem typu NAS typ B".
24	Każde z rozwiązań pamięci masowej musi zapewniać synchronizacje shareów SMB oraz NFS między ośrodkiem podstawowym a zapasowym
25	Każde z rozwiązań pamięci masowej musi zapewnić automatyczną detekcje zmian na określonych share'ach czy exportach (SMB,NFS) dotyczącą zabezpieczeń oraz synchronizacji.
26	Rozwiązanie pamięci dyskowej musi zawierać funkcjonalność deduplikacji na poziomie bloków o wielkości nie większej, niż 8KiB dla wyznaczonych katalogów.
27	Rozwiązanie pamięci dyskowej musi umożliwiać wykonanie kopii migawkowej (snapshot).
28	Administracja systemem musi odbywać się poprzez Web GUI oraz Command Line Interface.
29	Rozwiązanie musi zapewniać dostęp do danych przy jednoczesnym wykorzystaniu portów/interfejsów typu 10 Gigabit Ethernet.
30	Rozwiązanie pamięci dyskowej musi posiadać nie mniej niż 38 portów typu 10 Gigabit Ethernet. Sumaryczna przepustowość portów zapewniających dostęp do danych (od strony serwerów i sieci LAN) musi być nie mniejsza niż 380 Gbps.
31	System pamięci masowej musi zapewnić zdalny monitoring w celu diagnozy i usuwania usterek oraz w zakresie konserwacji – musi mieć możliwość automatycznej diagnozy i samodzielnego zgłaszania usterek w centrum serwisowym producenta.
32	Komunikacja pomiędzy kontrolerami/półkami dyskowymi musi odbywać się za pośrednictwem osobnych (niewspółdzielonych z portami dostępowymi) interfejsów. Każdy kontroler musi posiadać interfejsy o łącznej przepustowości nie mniejszej, niż 40Gbitps/kontroler.
33	Urządzenie musi zapewniać przegląd statystyk historycznych jak i w czasie rzeczywistym w postaci graficznych raportów w zakresie: • Wydajności: klastra, dysków, kontrolerów, portów Ethernet oraz systemu plików rozbiciu na ścieżkę dostępu. • Użycia systemu plików: użycie pojemności klastra oraz prognoza użycia, histogram wielkości składowanych plików, lista plików o największym rozmiarze, najstarszych w sensie utworzenia, dostępu, modyfikacji. Należy dostarczyć licencję na cała pojemność systemu.
34	Rozwiązanie pamięci dyskowej pozwala na ochronę wybranych danych przed ich utratą.
35	Rozwiązanie pamięci dyskowej oferuje zabezpieczenie chroniące je przed jednoczesną utratą minimalnie 4 dowolnych dysków lub 4 dowolnych półek dyskowych(węzłów) jednocześnie oferując mirroring określonych katalogów i plików od 1x do 8x.
36	Rozwiązanie pamięci masowej musi obsługiwać REST APIs (Restull Access to Namespace) dla aplikacji zewnętrznych.
37	Rozwiązanie pamięci masowej musi mieć możliwość rozbudowy o mechanizmy dotyczące szyfrowania danych oraz bezpieczeństwa umożliwiające spełnienie *standardów* HIPPA, PCI DSS,

	FIPS 140-2.
38	System pamięci masowej musi mieć możliwość skalowania pojemności zachowując pełny dostęp do danych i bez konieczności ich manualnej migracji na nowo przyłączane dyski/półki w celu ich redystrybucji.
39	"Rozwiązaniem typu NAS typ A" musi posiadać dedykowane oprogramowanie z portfolio produktu pamięci masowej służące do replikacji z oferowanym "rozwiązaniem typu NAS typ B".
40	System plików zaproponowanego rozwiązania zapewnia dostęp dla nieograniczonej liczby klientów bez względu na rodzaj użytego protokołu czy systemu operacyjnego.
41	System pamięci masowej opiera się na zabezpieczeniu danych znajdujących się na dyskach takim, aby zachować dostępu do danych w przypadku awarii, co najmniej trzech dowolnych półek dyskowych jednocześnie, albo trzech dowolnych dysków.

9.4.2 Rozwiązanie NAS typ B - 1szt.

Produkt musi spełnić następujące wymagania:

9.4.2.1 Wymagania ogólne

ID	Wymaganie
1	Pojemność użyteczna oferowanego rozwiązania pamięci dyskowej na dane użytkowników musi wynosić nie mniej niż 2100 TiB w obrębie jednego systemu plików przy zachowaniu dostępu do danych w przypadku awarii, co najmniej trzech dowolnych dysków jednocześnie, lub jednoczesnej awarii dysku i półki.
2	Pojemność ma być zbudowana na dyskach NLSAS oraz dyskach SSD nie mniejszych niż 1.6TB.
3	Rozwiązanie pamięci masowej musi posiadać co najmniej 10 kontrolerów gdzie każdy realizuje dostęp plikowy do danych.
4	Rozwiązanie musi umożliwiać rozbudowę, do co najmniej 16 kontrolerów w ramach tego samego systemu dyskowego.
5	Dla maksymalizacji gęstości, tj. minimalizacji wykorzystania obszaru serwerowni do przechowywania danych, półka dyskowa lub węzeł stanowiący element rozwiązania pamięci dyskowej musi mieścić nie mniej, niż 6 dysków typu NL-SAS lub SAS w przeliczeniu na 1U (tj. np. nie mniej, niż 24 dyski w obudowie 4U).
6	Rozwiązanie pamięci dyskowej musi udostępniać całkowitą dostępną przestrzeń w ramach jednego ciągłego systemu plików.
7	Rozwiązanie pamięci dyskowej musi zapewniać dostępną, łączną pojemność pamięci cache typu RAM nie mniejszą niż 480 GB. Ze względu na przewidywane obciążenie i wymaganą wydajność nie dopuszcza się realizacji pamięci w oparciu o dyski SSD.

ID	Wymaganie
8	Oferowane rozwiązanie musi zawierać nie mniej niż 10 dysków SSD o pojemności nie mniejszej niż 1.6TB każdy. Dyski SSD muszą być wykorzystywane do zwiększenia wydajności całości rozwiązania.
9	Rozwiązanie pamięci dyskowej musi zapewniać pracę jednocześnie wszystkich kontrolerów w trybie aktywny/aktywny dla zapewnienia niezawodności i dostępności danych.
10	Musi umożliwiać zwiększenie trzykrotne pojemności bez wprowadzania zmian do zaproponowanych kontrolerów.
11	Oferowane urządzenie musi umożliwiać dynamiczne rozszerzanie pojemności systemu plików w oparciu o całą pojemność fizyczną dodawaną do klastra bez konieczności: - modyfikacji już zainstalowanych kontrolerów, - restartu systemu, - ręcznej migracji/dystrybucji danych na nowe dyski systemu.
12	System plików zawarty w oferowanym rozwiązaniu musi być skalowalny, do co najmniej 30 PiB powierzchni netto.
13	Rozwiązanie pamięci masowej musi zapewniać dostęp z różnych systemów operacyjnych (UNIX, Mac, Linux, Windows) z wykorzystaniem wszystkich standardowych protokołów: NFS, SMB (CIFS), FTP. Wszystkie protokoły muszą być włączone bez dodatkowych licencji i sprzętu.
14	Rozwiązanie pamięci masowej musi obsługiwać protokoły plikowe: NFS V3 i V4, CIFS 2.0 i 3.0, FTP.
15	Oferowane rozwiązanie pamięci dyskowej musi obsługiwać protokół NDMP w wersji 4 dla kopii zapasowych na taśmach, z dowolnego obszaru systemu plików.
16	Oferowane rozwiązanie pamięci dyskowej musi zapewnić gwarantowaną ochronę przed „cichym uszkodzeniem dysków” (silent data corruption) dla wszystkich technologii dyskowych (w tym SATA).
17	Rozwiązanie musi zapewniać wsparcie dla SMB multi-channel pozwalając na korzystanie z kilku kanałów komunikacji dla zwiększenia przepustowości, tolerancje awarii jednego z połączeń I automatycznego wychwycenia tego typu awarii.
18	Oferowane rozwiązanie pamięci dyskowej musi umożliwiać wymianę uszkodzonego dysku przy zachowaniu nieprzerwanej dostępności wszystkich zasobów, tj. bez czasowego wyłączania z użycia innych elementów urządzenia. Musi istnieć możliwość jasnego określenia lokalizacji uszkodzonego dysku, np. za pomocą lampki kontrolnej lub wyświetlenia numeru pojedynczej zatoki/kieszeni.
19	W przypadku awarii jednego dysku, czas od momentu jego wymiany do odzyskania pierwotnego poziomu ochrony danych nie może być dłuższy niż 12 godzin – w sytuacji braku obciążenia przez urządzenia klienckie.
20	Rozwiązanie pamięci dyskowej musi zapewniać pracę jednocześnie wszystkich kontrolerów w trybie aktywny/aktywny dla zapewnienia niezawodności i dostępności danych.

ID	Wymaganie
21	Użytkownicy sieci muszą uzyskiwać dostęp do systemu pamięci masowej przy wykorzystaniu wewnętrznego load balancingu bez konieczności stosowania zewnętrznych urządzeń równoważących obciążenie. Powyższe wymaganie nie dotyczy rozwiązań opartych na dwóch kontrolerach.
22	Rozwiązanie pamięci dyskowej musi posiadać funkcjonalność replikacji asynchronicznej danych.
23	Rozwiązanie pamięci masowej musi realizować replikację asynchroniczną danych na poziomie pojedynczego katalogu celem dystrybucji treści i zapewnienia kopii danych w innym ośrodku.
24	Rozwiązanie pamięci masowej musi zapewniać synchronizacje shareów SMB oraz NFS między oferowanym "rozwiązaniem typu NAS typ A" a "rozwiązaniem typu NAS typ B".
25	Rozwiązanie pamięci masowej musi zapewnić automatyczną detekcje zmian na określonych share'ach czy exportach (SMB,NFS) dotyczącą zabezpieczeń oraz synchronizacji.
26	Rozwiązanie pamięci dyskowej musi umożliwiać wykonanie kopii migawkowej (snapshot).
27	Rozwiązanie pamięci dyskowej musi zawierać funkcjonalność deduplikacji na poziomie bloków o wielkości nie większej, niż 8KiB dla wyznaczonych katalogów.
28	Rozwiązanie pamięci masowej musi posiadać mechanizm równoważenia nowych połączeń pomiędzy kontrolerami zgodnie z polityką wyboru kontrolera: kontroler o najmniejszej liczbie połączeń, kontroler o najmniejszym wykorzystaniu CPU, polityka roundrobin. Powyższe wymaganie nie dotyczy rozwiązań opartych na dwóch kontrolerach.
29	Administracja systemem musi odbywać się poprzez Web GUI oraz Command Line Interface.
30	Rozwiązanie musi zapewniać dostęp do danych przy jednoczesnym wykorzystaniu portów/interfejsów typu 10 Gigabit Ethernet.
31	Rozwiązanie pamięci masowej musi posiadać nie mniej niż 20 portów typu 10 Gigabit Ethernet. Sumaryczna przepustowość portów zapewniających dostęp do danych (od strony serwerów i sieci LAN) musi być nie mniejsza niż 200 Gbps.
32	Komunikacja pomiędzy kontrolerami/półkami dyskowymi musi odbywać się za pośrednictwem osobnych (niewspółdzielonych z portami dostępowymi) interfejsów. Każdy kontroler musi posiadać interfejsy o łącznej przepustowości nie mniejszej, niż 20Gbitps/kontroler. Sumaryczna przepustowość interfejsów wszystkich kontrolerów musi być nie mniejsza, niż 200Gbitps.
33	Urządzenie musi zapewniać przegląd statystyk historycznych jak i w czasie rzeczywistym w postaci graficznych raportów w zakresie: • Wydajności: klastra, dysków, kontrolerów, portów Ethernet oraz systemu plików rozbiciu na ścieżkę dostępu. • Użycia systemu plików: użycie pojemności klastra oraz prognoza użycia, histogram wielkości składowanych plików, lista plików o największym rozmiarze, najstarszych w sensie utworzenia, dostępu, modyfikacji. Należy dostarczyć licencję na cała pojemność systemu.

ID	Wymaganie
34	Rozwiązanie pamięci masowej musi zapewnić zdalny monitoring w celu diagnozy i usuwania usterek oraz w zakresie konserwacji – musi mieć możliwość automatycznej diagnozy i samodzielnego zgłaszania usterek w centrum serwisowym producenta.
35	Rozwiązanie pamięci dyskowej pozwala na ochronę wybranych danych przed ich utratą.
36	Rozwiązanie pamięci dyskowej oferuje zabezpieczenie chroniące je przed jednoczesną utratą minimalnie 4 dowolnych dysków lub czterech dowolnych półek dyskowych(węzłów) jednocześnie oferując mirroring określonych katalogów i plików od 1x do 8x.
37	Rozwiązanie pamięci masowej musi obsługiwać REST APIs (Restull Access to Namespace) dla aplikacji zewnętrznych.
38	Rozwiązanie pamięci masowej musi mieć możliwość rozbudowy o mechanizmy dotyczące szyfrowania danych oraz bezpieczeństwa umożliwiające spełnienie *standardów* HIPPA, PCI DSS, FIPS 140-2.
39	System pamięci masowej musi mieć możliwość skalowania pojemności zachowując pełny dostęp do danych i bez konieczności ich manualnej migracji na nowo przyłączane dyski/półki w celu ich redystrybucji.
40	"Rozwiązaniem typu NAS typ B" musi posiadać dedykowane oprogramowanie z portfolio produktu pamięci masowej służące do replikacji z oferowanym "rozwiązaniem typu NAS typ A".
41	System plików zaproponowanego rozwiązania zapewnia dostęp dla nieograniczonej liczby klientów bez względu na rodzaj użytego protokołu czy systemu operacyjnego.
42	System pamięci masowej opiera się na zabezpieczeniu danych znajdujących się na dyskach takim, aby zachować dostępu do danych w przypadku awarii, co najmniej trzech dowolnych dysków jednocześnie, lub jednoczesnej awarii dysku i półki.

9.4.3 Rozwiązanie NAS typ C - 1szt.

Urządzenie fizycznie do zainstalowania w Katowicach.
Produkt musi spełnić następujące wymagania:

9.4.3.1 Wymagania ogólne

ID	Wymaganie
1	Pojemność użyteczna oferowanego rozwiązania pamięci dyskowej na dane użytkowników musi wynosić nie mniej niż 2300 TiB w obrębie jednego systemu plików przy zachowaniu dostępu do danych w przypadku awarii, co najmniej trzech dowolnych dysków jednocześnie, lub jednoczesnej awarii dysku i półki.
2	Pojemność ma być zbudowana na dyskach NLSAS oraz dyskach SSD nie mniejszych niż 1.6TB.

ID	Wymaganie
3	Rozwiązanie pamięci masowej musi zawierać, co najmniej 10 kontrolerów gdzie każdy realizuje dostęp plikowy do danych.
4	Rozwiązanie pamięci masowej musi umożliwiać rozbudowę, do co najmniej 16 kontrolerów w ramach tego samego systemu dyskowego.
5	W celu zapewnienia odpowiedniej wydajności oferowany system pamięci masowej musi posiadać nie mniej niż 7 CPU.
6	Dla maksymalizacji gęstości, tj. minimalizacji wykorzystania obszaru serwerowni do przechowywania danych, półka dyskowa lub węzeł stanowiący element rozwiązania pamięci dyskowej musi mieścić nie mniej, niż 6 dysków typu NL-SAS lub SAS w przeliczeniu na 1U (tj. np. nie mniej, niż 24 dysków w obudowie 4U).
7	Rozwiązanie pamięci dyskowej musi udostępniać całkowitą dostępną przestrzeń w ramach jednego ciągłego systemu plików.
8	Rozwiązanie pamięci masowej musi zapewniać dostępną, łączną pojemność pamięci cache typu RAM nie mniejszą niż 336 GB. Ze względu na przewidywane obciążenie i wymaganą wydajność nie dopuszcza się realizacji pamięci w oparciu o dyski SSD.
9	Oferowane rozwiązanie musi zawierać nie mniej niż 10 dysków SSD o pojemności nie mniejszej niż 1.6TB każdy. Dyski SSD muszą być wykorzystywane do zwiększenia wydajności całości rozwiązania.
10	Rozwiązanie pamięci masowej musi umożliwiać zwiększenie trzykrotne pojemności bez wprowadzania zmian do zaproponowanych kontrolerów.
11	Oferowane rozwiązanie pamięci masowej musi umożliwiać dynamiczne rozszerzanie pojemności systemu plików w oparciu o całą pojemność fizyczną dodawaną do klastra bez konieczności: - modyfikacji już zainstalowanych kontrolerów - restartu systemu - ręcznej migracji/dystrybucji danych na nowe dyski systemu.
12	Rozwiązanie pamięci masowej musi zapewniać dostęp z różnych systemów operacyjnych (UNIX, Mac, Linux, Windows) z wykorzystaniem wszystkich standardowych protokołów: NFS, SMB (CIFS), HTTP, FTP. Wszystkie protokoły muszą być włączone bez dodatkowych licencji i sprzętu.
13	Rozwiązanie pamięci masowej musi obsługiwać protokoły plikowe: NFS V3 i V4, CIFS 2.0 i 3.0, FTP, http.
14	Rozwiązanie musi zapewniać wsparcie dla SMB multi-channel pozwalając na korzystanie z kilku kanałów komunikacji dla zwiększenia przepustowości, tolerancje awarii jednego z połączeń I automatycznego wychwycenia tego typu awarii.
15	Oferowane rozwiązanie pamięci dyskowej musi obsługiwać protokół NDMP w wersji 4 dla kopii zapasowych na taśmach, z dowolnego obszaru systemu plików.
16	Oferowane rozwiązanie pamięci dyskowej musi zapewnić gwarantowaną ochronę przed „cichym uszkodzeniem dysków” (silent data corruption) dla wszystkich technologii dyskowych (w tym

ID	Wymaganie
	SATA).
17	Oferowane rozwiązanie pamięci dyskowej musi umożliwiać wymianę uszkodzonego dysku przy zachowaniu nieprzerwanej dostępności wszystkich zasobów, tj. bez czasowego wyłączania z użycia innych elementów urządzenia. Musi istnieć możliwość jasnego określenia lokalizacji uszkodzonego dysku, np. za pomocą lampki kontrolnej lub wyświetlenia numeru pojedynczej zatoki/kieszeni.
18	W przypadku awarii jednego dysku, czas od momentu jego wymiany do odzyskania pierwotnego poziomu ochrony danych nie może być dłuższy niż 12 godzin – w sytuacji braku obciążenia przez urządzenia klienckie.
19	Rozwiązanie pamięci dyskowej musi zapewniać pracę jednocześnie wszystkich kontrolerów w trybie aktywny/aktywny dla zapewnienia niezawodności i dostępności danych.
20	Użytkownicy sieci muszą uzyskiwać dostęp do systemu pamięci masowej przy wykorzystaniu wewnętrznego load balancingu bez konieczności stosowania zewnętrznych urządzeń równoważących obciążenie. Powyższe wymaganie nie dotyczy rozwiązań opartych na dwóch kontrolerach.
21	Rozwiązanie pamięci dyskowej musi posiadać funkcjonalność replikacji asynchronicznej danych.
22	Rozwiązanie pamięci masowej musi realizować replikację asynchroniczną danych na poziomie pojedynczego katalogu celem dystrybucji treści i zapewnienia kopii danych z oferowanym "rozwiązaniem typu NAS typ B".
23	Rozwiązanie pamięci masowej musi zapewniać synchronizacje shareów SMB oraz NFS między oferowanym "rozwiązaniem typu NAS typ B" a "rozwiązaniem typu NAS typ C"
24	Rozwiązanie pamięci masowej musi zapewnić automatyczną detekcje zmian na określonych share'ach czy exportach (SMB,NFS) dotyczącą zabezpieczeń oraz synchronizacji.
25	Rozwiązanie pamięci dyskowej musi umożliwiać wykonanie, co najmniej 1000 kopii migawkowych (snapshot) danego katalogu oraz umożliwiać wykonanie nielimitowanej liczby kopii migawkowych w odniesieniu do całego systemu plików.
26	Komunikacja pomiędzy kontrolerami/półkami dyskowymi musi odbywać się za pośrednictwem osobnych (niewspółdzielonych z portami dostępowymi) interfejsów. Każdy kontroler musi posiadać interfejsy o łącznej przepustowości nie mniejszej, niż 20Gbitps/kontroler. Sumaryczna przepustowość interfejsów wszystkich kontrolerów musi być nie mniejsza, niż 140Gbitps.
27	Rozwiązanie pamięci masowej musi zapewnić zdalny monitoring w celu diagnozy i usuwania usterek oraz w zakresie konserwacji – musi mieć możliwość automatycznej diagnozy i samodzielnego zgłaszania usterek w centrum serwisowym producenta.
28	Administracja systemem musi odbywać się poprzez Web GUI oraz Command Line Interface.
29	Zapewniać dostęp do danych przy jednoczesnym wykorzystaniu portów/interfejsów typu 10 Gigabit Ethernet.

ID	Wymaganie
30	Rozwiązanie pamięci dyskowej posiadać nie mniej niż 14 portów typu 10 Gigabit Ethernet. Sumaryczna przepustowość portów zapewniających dostęp do danych (od strony serwerów i sieci LAN) musi być nie mniejsza niż 140 Gbps.
31	Urządzenie musi zapewniać przegląd statystyk historycznych jak i w czasie rzeczywistym w postaci graficznych raportów w zakresie: • Wydajności: klastra, dysków, kontrolerów, portów Ethernet oraz systemu plików rozbiciu na ścieżkę dostępu. • Użycia systemu plików: użycie pojemności klastra oraz prognoza użycia, histogram wielkości składowanych plików, lista plików o największym rozmiarze, najstarszych w sensie utworzenia, dostępu, modyfikacji. Należy dostarczyć licencję na cała pojemność systemu.
32	Rozwiązanie pamięci dyskowej pozwala na ochronę wybranych danych przed ich utratą.
33	Rozwiązanie pamięci dyskowej oferuje zabezpieczenie chroniące je przed jednoczesną utratą minimalnie 4 dowolnych dysków lub czterech dowolnych półek dyskowych(węzłów) jednocześnie oferując mirroring określonych katalogów i plików od 1x do 8x.
34	Rozwiązanie pamięci masowej musi obsługiwać REST APIs (Restull Access to Namespace) dla aplikacji zewnętrznych.
35	Rozwiązanie pamięci masowej musi mieć możliwość rozbudowy o mechanizmy dotyczące szyfrowania danych oraz bezpieczeństwa umożliwiające spełnienie *standardów* HIPPA, PCI DSS, FIPS 140-2.
36	System pamięci masowej musi mieć możliwość skalowania pojemności zachowując pełny dostęp do danych i bez konieczności ich manualnej migracji na nowo przyłączane dyski/półki w celu ich redystrybucji.
37	"Rozwiązaniem typu NAS typ C" musi posiadać dedykowane oprogramowanie z portfolio produktu pamięci masowej służące do replikacji z oferowanym "rozwiązaniem typu NAS typ B".
38	System plików zaproponowanego rozwiązania zapewnia dostęp dla nieograniczonej liczby klientów bez względu na rodzaj użytego protokołu czy systemu operacyjnego.
39	System pamięci masowej opiera się na zabezpieczeniu danych znajdujących się na dyskach takim, aby zachować dostępu do danych w przypadku awarii, co najmniej trzech dowolnych dysków jednocześnie, lub jednoczesnej awarii dysku i półki.
40	Należy dostarczyć switch LAN zapewniający komunikację wewnątrz całości rozwiązania oraz dodatkowo minimum 2 porty 10 Gigabit Ethernet i 2 porty 1 Gigabit Ethernet wraz z odpowiednimi wkładkami, do połączenia z posiadaną w lokalizacji infrastrukturą LAN.
41	Należy dostarczyć dobrany do całości rozwiązania zasilacz UPS, z podtrzymaniem zasilania na minimum 10 minut dla dostarczonego "rozwiązania typu NAS typ C".
42	Wraz z rozwiązaniem należy dostarczyć szafę RACK 42U, z odpowiednimi modułami zasilającymi

ID	Wymaganie
	PDU, do której należy zainstalować całość dostarczonego "rozwiązania typu NAS typ C".

9.5 Switch SAN – 2 szt.

Produkt musi spełnić następujące wymagania:

9.5.1 Wymagania ogólne

ID	Wymaganie
1	Przełącznik FC musi być wykonany w technologii FC minimum 16 Gb/s i zapewniać możliwość pracy portów FC z prędkościami 16, 8, 4, 2 Gb/s w zależności od rodzaju zastosowanych wkładek SFP. W przypadku obsadzenia portu FC za pomocą wkładki SFP 16Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 16, 8 lub 4 Gb/s, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji.
2	W przypadku obsadzenia portu FC za pomocą wkładki SFP 8Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 8, 4 lub 2 Gb/s, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji.
3	Przełącznik FC musi być wyposażony, w co najmniej 36 aktywnych portów FC obsadzonych wkładkami SFP 16Gb/s.
4	Wszystkie zaoferowane porty przełącznika FC muszą umożliwiać działanie bez tzw. oversubscrypcji gdzie wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika mogą pracować równocześnie z pełną prędkością 8Gb/s lub 16Gb/s w zależności do zastosowanych wkładek FC.
5	Całkowita przepustowość przełącznika FC dostępna dla maksymalnie rozbudowanej konfiguracji wyposażonej we wkładki 16Gb/s musi wynosić minimum 1536 Gb/s end-to-end full duplex.
6	Oczekiwana wartość opóźnienia przy przesyłaniu ramek FC między dowolnymi portami przełącznika nie może być większa niż 1,2µs.
7	Rodzaj obsługiwanych portów, co najmniej: E, D oraz F.
8	Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) i szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”.
9	Przełącznik FC posiadać nadmiarowe zasilacze i wentylatory, których wymiana musi być możliwa w trybie „na gorąco” bez przerywania pracy przełącznika.
10	Przełącznik FC musi mieć możliwość agregacji połączeń ISL między dwoma przełącznikami i tworzenia w ten sposób logicznych połączeń typu trunk o przepustowości minimum 128 Gb/s dla każdego logicznego połączenia. Load balancing ruchu między fizycznymi połączeniami ISL w ramach połączenia logicznego typu trunk musi być realizowany na poziomie pojedynczych ramek FC a połączenie logiczne musi zachowywać kolejność przesyłanych ramek.

11	Przełącznik FC musi wspierać mechanizm balansowania ruchu, pomiędzy co najmniej 6 różnymi połączeniami o tym samym koszcie wewnątrz wielodomenowych sieci fabric, przy czym balansowanie ruchu musi odbywać się w oparciu o 3 parametry nagłówka ramki FC: DID, SID i OXID.
12	Przełącznik FC musi zapewniać jednoczesną obsługę mechanizmów ISL Trunk oraz balansowania ruchu w oparciu o DID/SID/OXID. Jednoczesne wykorzystanie obu mechanizmów powinno zapewnić dla dowolnej pary komunikujących się urządzeń końcowych uzyskanie kanału komunikacyjnego o zagregowanej przepustowości 768Gb/s half duplex.
13	Przełącznik FC musi realizować sprzętową obsługę zoningu (przez tzw. układ ASIC) na podstawie portów i adresów WWN.
14	Przełącznik FC musi mieć możliwość wymiany i aktywacji wersji firmware'u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia i bez zakłócenia przesyłanego ruchu FC.
15	Przełącznik FC musi wspierać następujące mechanizmy zwiększające poziom bezpieczeństwa: • mechanizm szyfrowania i kompresji wybranych połączeń ISL wspierany, na co najmniej 2 portach przełącznika FC. Symetryczny klucz szyfrujący nie może być krótszy niż 256-bitów. • mechanizm tzw. Fabric Binding, który umożliwia zdefiniowanie listy kontroli dostępu regulującej prawa przełączników FC do uczestnictwa w sieci fabric • uwierzytelnianie (autentykacja) przełączników w sieci Fabric za pomocą protokołów DH-CHAP i FCAP • uwierzytelnianie (autentykacja) urządzeń końcowych w sieci Fabric za pomocą protokołu DH-CHAP • szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2. • definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control) • definiowane kont administratorów w środowisku RADIUS i LDAP • szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS • obsługa SNMP v1 oraz v3 • IP Filter dla portu administracyjnego przełącznika • wgrywanie nowych wersji firmware przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP • wykonywanie kopii bezpieczeństwa konfiguracji przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP
16	Przełącznik FC musi mieć możliwość konfiguracji przez: • polecenia tekstowe w interfejsie znakowym konsoli terminala, • przeglądarkę internetową z interfejsem graficznym lub dedykowane oprogramowanie.

17	Przełącznik FC musi być wyposażony w następujące narzędzia diagnostyczne i mechanizmy obsługi ruchu FC: • logowanie zdarzeń poprzez mechanizm „syslog”, • port diagnostyczny tzw. D_port. Port diagnostyczny musi umożliwiać wykonanie testów sprawdzających komunikację portu przełącznika z wkładką SFP, połączenie optyczne pomiędzy dwoma przełącznikami oraz pomiar opóźnienia i odległości między przełącznikami z dokładnością do 5m dla wkładek SFP 16Gbps. Testy wykonywane przez port diagnostyczny nie mogą wpływać w żaden sposób na działanie pozostałych portów przełącznika i całej sieci fabric. • FC ping • FC traceroute • kopiowanie danych wymienianych pomiędzy dwoma wybranymi portami na inny wybrany port przełącznika.
18	Przełącznik FC musi mieć możliwość instalacji wkładek SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 25km z prędkością 8Gb/s.
19	Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC.
20	Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S.
21	W przełączniku FC musi istnieć możliwość wydzielenia logicznych, izolowanych od siebie przełączników. Każdy z logicznych przełączników musi mieć własny Domain ID, własne usługi fabric (tzw. fabric services), niezależną bazę zoningu oraz możliwość przypisanie dedykowanego administratora.
22	Musi istnieć możliwość połączenia wybranych logicznych przełączników wydzielonych w różnych fizycznych przełącznikach FC za pomocą dedykowanych połączeń ISL. Połączone w ten sposób przełączniki muszą tworzyć pojedynczą sieć fabric.
23	Wsparcie dla N_Port ID Virtualization (NPIV). Obsługa, co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika.
24	Przełącznik FC musi obsługiwać protokół FCP na dowolnych portach przełącznika.

9.6 Oprogramowanie do wirtualizacji serwerów

Rozbudowa posiadanego przez Zamawiającego środowiska do wirtualizacji VMware vSphere Enterprise plus o licencje na 28 procesorów wraz z jedną centralną konsolą do zarządzania całym środowiskiem wirtualizacji, lub równoważne.

Wszystkie licencje mają być dostarczone wraz z wsparciem technicznym, z czasem trwania wsparcia technicznego, zgodnym z ofertą Wykonawcy - „Czas Trwania Wsparcia Technicznego”, świadczonym przez producenta będącego licencjodawcą oprogramowania, które powinno umożliwiać zgłaszanie problemów 5 dni w tygodniu przez 12h na dobę oraz pobieranie i instalowanie nowych poprawek, wersji oprogramowania.

	Oprogramowanie ma spełniać następujące minimalne wymagania równoważności:
ID	Wymaganie
1	Warstwa wirtualizacji musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym i nie może być częścią innego systemu operacyjnego.
2	Warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 200MB pamięci operacyjnej RAM serwera fizycznego.
3	Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym. Wymagana jest możliwość przydzielenia maszynie większej ilości wirtualnej pamięci operacyjnej niż jest zainstalowana w serwerze fizycznym oraz większej ilości przestrzeni dyskowej niż jest fizycznie dostępna.
4	Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością dostępu do 4TB pamięci operacyjnej.
5	Oprogramowanie do wirtualizacji musi zapewnić możliwość przydzielenia maszynom wirtualnym do 128 procesorów wirtualnych.
6	Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
7	Rozwiązanie musi w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
8	Rozwiązanie musi wspierać następujące systemy operacyjne: Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, SLES 11, SLES 10, SLES9, Ubuntu, RHEL 5, RHEL 4, RHEL3. Solaris wersja 10 dla platformy x86, Debian, CentOS, FreeBSD, SCO OpenServer, SCO Unixware.
9	Rozwiązanie musi zapewniać sprzętowe wsparcie dla wirtualizacji zagnieżdżonej, w szczególności w zakresie możliwości zastosowania trybu XP mode w Windows 7 a także instalacji wszystkich funkcjonalności w tym Hyper-V pakietu Windows Server 2012 na maszynie wirtualnej.
10	Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania środowiskiem serwerów wirtualnych. Konsola graficzna musi być dostępna poprzez dedykowanego klienta i za pomocą przeglądarek, minimum IE i Firefox.
11	Dostęp przez przeglądarkę do konsoli graficznej musi być skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska.
12	Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta root.
13	Rozwiązanie musi zapewnić możliwość monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej i zdefiniowania alertów informujących o przekroczeniu wartości progowych.

14	Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji.
15	Rozwiązanie musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi.
16	Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii zapasowych instancji systemów operacyjnych oraz ich odtworzenia w możliwie najkrótszym czasie.
17	Kopie zapasowe muszą być składowane z wykorzystaniem technik de-duplikacji danych.
18	Musi istnieć możliwość odtworzenia pojedynczych plików z kopii zapasowej maszyny wirtualnej przez osoby do tego upoważnione bez konieczności nadawania takim osobom bezpośredniego dostępu do głównej konsoli zarządzającej całym środowiskiem.
19	Mechanizm zapewniający kopie zapasowe musi być wyposażony w system cyklicznej kontroli integralności danych. Ponadto musi istnieć możliwość przywrócenia stanu repozytorium kopii zapasowych do punktu w czasie, kiedy wszystkie dane były integralne w przypadku jego awarii.
20	Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością wskazania konieczności zachowania stanu pamięci pracującej maszyny wirtualnej.
21	Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
22	Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności: Microsoft Active Directory, Open LDAP.
23	Platforma wirtualizacyjna musi umożliwiać zastosowanie w serwerach fizycznych procesorów o dowolnej ilości rdzeni.
24	Rozwiązanie musi umożliwiać tworzenie jednorodnych wolumenów logicznych o wielkości do 62TB.
25	Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej.
26	Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
27	Rozwiązanie musi umożliwiać wykorzystanie technologii 10GbE w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi.

28	Rozwiązanie musi zapewniać możliwość replikacji maszyn wirtualnych z dowolnej pamięci masowej w tym z dysków wewnętrznych serwerów fizycznych na dowolną pamięć masową w tym samym lub oddalonym ośrodku przetwarzania.
29	Rozwiązanie musi gwarantować współczynnik RPO na poziomie minimum 5 minut
30	Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum.
31	Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.
32	Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.
33	System musi mieć możliwość uruchamiania fizycznych serwerów z centralnie przygotowanego obrazu poprzez protokół PXE.
34	Rozwiązanie musi umożliwiać utworzenie jednorodnego, wirtualnego przełącznika sieciowego, rozproszonego na wszystkie serwery fizyczne platformy wirtualizacyjnej. Przełącznik taki musi zapewniać możliwość konfiguracji parametrów sieciowych maszyny wirtualnej z granulacją na poziomie portu tego przełącznika. Pojedyncza maszyna wirtualna musi mieć możliwość wykorzystania jednego lub wielu portów przełącznika z niezależną od siebie konfiguracją.
35	Konsola zarządzania platformą wirtualizacji musi umożliwiać centralną konfigurację przełącznika rozproszonego a mechanizmy wewnętrzne muszą zapewniać propagację tej konfiguracji do wszystkich serwerów fizycznych tworzących wzajemnie ten przełącznik.
36	Platforma wirtualizacji powinna w ramach przełącznika sieciowego musi zapewniać możliwość integracji z produktami (przełącznikami wirtualnymi) firm trzecich, tak aby umożliwić granularną delegację zadań w zakresie zarządzania konfiguracją sieci do zespołów sieciowych.
37	Przełącznik rozproszony musi współpracować z protokołem NetFlow.
38	Przełącznik rozproszony musi umożliwiać funkcjonalność duplikowania ruchu sieciowego dowolnego jego portu wirtualnego na inny port.
39	Przełącznik musi mieć wbudowane mechanizmy składowania kopii konfiguracji, przywracania tej kopii a także mechanizmy automatycznie zapobiegające niewłaściwej konfiguracji sieciowej, które w całości lub w części mogą eliminować błędy ludzkie i utratę łączności sieciowej.
40	System musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowane wirtualne urządzenia dedykowane dla poszczególnych maszyn wirtualnych.
41	Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi, pamięciami masowymi niezależnie od dostępności współdzielonej przestrzeni dyskowej, różnymi rodzajami virtualnych przełączników sieciowych, pomiędzy Centrami Przetwarzania Danych oraz pomiędzy Centralnymi

	Konsolami Zarządzającymi platformami wirtualnymi.
42	Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały automatycznie przełączone na inne serwery infrastruktury.
43	Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury.
44	Rozwiązanie musi zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania.
45	Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacje wliczając w to zarówno poprawki bezpieczeństwa jaki zmianę jej wersji.
46	Rozwiązanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci.
47	Decyzja o próbie przywrócenia funkcjonalności maszyny wirtualnej w przypadku awarii lub niedostępności serwera fizycznego powinna być podejmowana automatycznie, jednak musi istnieć możliwość określenia przez administratora czasu po jakim taka decyzja jest wykonywana.
48	Rozwiązanie musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (o maksymalnie czterech procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii serwerów fizycznych, bez utraty danych i dostępności danych podczas awarii serwerów fizycznych.
49	Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum. Konieczna jest możliwość przenoszenia usług pomiędzy serwerami fizycznymi, wolumenami dyskowymi, klastrami, centrami przetwarzania danych bez przerywania pracy usług.
50	Rozwiązanie musi umożliwiać automatyczne równoważenie obciążenia serwerów fizycznych pracujących jako platforma dla infrastruktury wirtualnej.
51	System musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu sieciowego oraz ustalania priorytetów w zależności od jego rodzaju na poziomie konkretnych maszyn wirtualnych.
52	System musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu do pamięci masowych oraz ustalania priorytetów dostępu do nich na poziomie konkretnych wirtualnych maszyn.
53	System musi mieć możliwość grupowania pamięci masowych o podobnych parametrach w grupy i przydzielania ich do wirtualnych maszyn zgodnie z ustaloną przez administratora polityką.

54	System musi mieć możliwość równoważenia obciążenia i zajętości pamięci masowych wraz z pełną automatyką i przenoszeniem plików wirtualnych maszyn z bardziej zajętych na mniej zajęte przestrzenie dyskowe lub/i z przestrzeni dyskowych bardziej obciążonych operacjami I/O na mniej obciążone.

9.7 Oprogramowanie do wirtualizacji sieci

Rozbudowa posiadanego przez Zamawiającego środowiska do wirtualizacji VMware vSphere Enterprise plus o licencje na wirtulizację warstwy sieciowej na 112 procesorów. Wszystkie licencje mają być wraz z wsparciem technicznym, z czasem trwania wsparcia technicznego, zgodnym z ofertą Wykonawcy - „Czas Trwania Wsparcia Technicznego", świadczonym przez producenta będącego licencjodawcą oprogramowania, które powinno umożliwiać zgłaszanie problemów 5 dni w tygodniu przez 12h na dobę oraz pobieranie i instalowanie nowych poprawek, wersji oprogramowania.

ID	Wymaganie
1	Rozwiązanie do wirtualizacji sieci musi zapewniać następujące usługi sieciowe: Wirtualny przełącznik, wirtualny router, wirtualny firewall, wirtualny load Balancer. Musi również dostarczać funkcję translacji adresów – NAT / PAT
2	Rozwiązanie musi zapewniać pełną funkcjonalność, niezależną od topologii sieci fizycznej i używanych w obrębie tej sieci w protokołów sieciowych.
3	Rozwiązanie musi być w pełni funkcjonalne dla obecnie działających aplikacji i w pełni gotowe do instalacji.
4	Rozwiązanie musi zapewniać pełną integrację z obecnie używanym przez Zamawiającego systemem do zarządzania wirtualnym środowiskiem VMware – Vcenter, oraz musi być w pełni wspierane przez producenta VMware.
5	Rozwiązanie musi zapewnić możliwość tworzenia segmentów sieci L2 i L3 na poziomie wirtualnej platformy, bez konieczności definiowania oraz modyfikacji konfiguracji fizycznych przełączników i routerów
6	Rozwiązanie musi dostarczać funkcji wirtualnej bramy domyślnej (default gateway) dla sieci zdefiniowanych na wirtualizatorze sieciowym.
7	Brama domyślna powinna działać w trybie rozproszonym i dostarczać możliwość przełączania pakietów L3 bezpośrednio na serwerze, bez konieczności przesyłania ruchu do fizycznych routerów.
8	Wirtualizacja segmentów L2 (virtual switch) musi być zintegrowana z hypervisorem na poziomie jądra (hypervisor kernel) oraz w pełni wspierana przez obecnego dostawcę hypervisora VMware.
9	Rozwiązanie musi zapewniać możliwość instalacji oraz zarządzania poprzez API
10	Rozwiązanie musi zapewniać bezpieczeństwo transmisji danych (filtracja pakietów) na poziomie hypervisora/wirtulanego interfejsu sieciowego (vNIC), dla całości transmisji danych (włączając w to transmisję pomiędzy wirtualnymi maszynami w tym samym wirtualnym

	segmencie sieci)
11	Rozwiązanie musi zapewniać usługę rozproszonego firewalla, typu stateful warstwy 4 na poziomie hypervisora/wirtulanego interfejsu sieciowego (vNIC)
12	Konstrukcja reguł bezpieczeństwa musi wspierać możliwość ich elastycznego oraz dynamicznego konstruowania poprzez wielopoziomową definicję obiektów np. nazwa maszyny wirtualnej, nazwa switcha wirtualnego, nazwa grupy maszyn wirtualnych – Security Group
13	Komponent rozwiązania platformy SDN powinien zawierać funkcję Wirtualnej Bramy, która zapewniać będzie szereg dodatkowych funkcji sieciowych.
14	Funkcją wirtualnej bramy musi być możliwość rozkładania ruchu – load balancing działającą do warstwy 7.
15	Wirtualna brama musi umożliwiać łączenie (bridging) środowiska zwirtualizowanego opartego o VXLAN oraz niezwirtualizowanego zdefiniowanego za pomocą VLANów
16	Jednym z komponentów BRAMY WIRTUALNEJ musi być funkcja wirtualnego routera wspierającego protokoły BGP i OSPF .
17	Rozwiązanie musi posiadać możliwość jednolitego zarządzania usługami sieciowymi dostępnymi w ramach platform wirtualizacji sieci :wirtualny switch, wirtualny router, wirtualny load balancer, wirtualny firewall
18	Rozwiązanie musi posiadać zarządzania politykami bezpieczeństwa poprzez API
19	Rozwiązanie musi oferować integrację z produktami firm trzecich (partnerskimi) i oferować następujące usługi w zakresie bezpieczeństwa zwirtualizowanej infrastruktury sieciowej: Firewall, IPS/IDS, Antyvirus, File Integrity Monitoring (FIM), Vulnerability Management

9.8 System operacyjny

Rozbudowa posiadanej przez Zamawiającego ilości licencji na system operacyjny MS Windows Server o licencje na 26 dostarczanych serwerów blade, lub równoważne.
Wszystkie licencje mają być dostarczone wraz z wsparciem technicznym, z czasem trwania wsparcia technicznego, zgodnym z ofertą Wykonawcy - „Czas Trwania Wsparcia Technicznego”, świadczonym przez producenta będącego licencjodawcą oprogramowania , które powinno umożliwiać zgłaszanie problemów 7 dni w tygodniu przez 24h na dobę wraz z prawem do pobierania i instalowania nowych wersji oprogramowania.

ID	Wymaganie
1	Dostarczane licencje muszą zapewniać możliwość korzystania z oprogramowania zainstalowanego na serwerze dla dowolnej liczby użytkowników zewnętrznych.

2	Dostarczone licencje nie mogą ograniczać liczby uruchomionych instancji systemu operacyjnego serwera.
3	System operacyjny musi być oparty o 64-bitową architekturę.
4	Licencja na system operacyjny musi być przypisana do każdego procesora fizycznego na serwerze.
5	Licencja musi uprawniać do uruchamiania nieograniczonej licencyjnie liczby serwerowego systemu operacyjnego w środowisku wirtualnym posiadanym przez Zamawiającego, dla zalicencjonowanych procesorów fizycznych serwera.
6	Możliwość wykorzystania co najmniej 2 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
7	Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
8	Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
9	Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
10	Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
11	Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
12	Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez instytucję lub firmę upoważnioną do wydawania certyfikatu bezpieczeństwa danych. Za równoważny Zamawiający uzna certyfikat potwierdzający bezpieczeństwo danych.
13	Możliwość uruchamiania aplikacji wykorzystujących technologię ASP.NET.
14	Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15	Graficzny interfejs użytkownika.
16	Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
17	Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
18	Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
19	Pochodzący od producenta systemu serwis zarządzania prawami do informacji

	w dokumentach (Digital Rights Management).
20	Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
21	Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
22	Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
23	Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
24	Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
25	Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe) z możliwością wykorzystania następujących funkcji: i. Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. c. Zdalna dystrybucja oprogramowania na stacje robocze, d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego umożliwiające: i. Dystrybucję certyfikatów poprzez http, ii. Konsolidację CA dla wielu lasów domen, iii. Automatyczne rejestrowanie certyfikatów pomiędzy różnymi lasami domen. f. Szyfrowanie plików i folderów, g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów, i. Serwis udostępniania stron WWW, j. Wsparcie dla protokołu IP w wersji 6 (IPv6), k. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows posiadanych przez Zamawiającego,

9.9 Oprogramowanie do ochrony antywirusowej

Rozbudowa posiadanego przez Zamawiającego oprogramowania do ochrony antywirusowej Trend Micro Deep Security - Anti-malware o licencje na 28 procesorów, lub równoważne. Wszystkie licencje mają być dostarczone wraz z wsparciem technicznym, z czasem trwania wsparcia technicznego, zgodnym z ofertą Wykonawcy - „Czas Trwania Wsparcia Technicznego", świadczonym przez producenta będącego licencjodawcą oprogramowania, które powinno umożliwiać zgłaszanie problemów 5 dni w tygodniu przez 12h na dobę oraz pobieranie i instalowanie nowych poprawek, sygnatur, wersji oprogramowania.

ID	Wymaganie
1	Oprogramowanie musi pozwalać na bezagentową ochronę środowisk wirtualnych opartych o platformę VMware vSphere.
2	Oprogramowanie musi zapewniać bezpieczeństwo wirtualnych serwerów.
3	Oprogramowanie musi umożliwiać instalację konsoli zarządzającej na systemach Microsoft Windows.
4	Oprogramowanie musi pozwalać na swobodny wybór ochrony agentowej lub bezagentowej w przypadku serwerów wirtualnych.
5	Administratorzy muszą mieć możliwość tworzenia logicznych grup klientów i serwerów, w celu zarządzania oraz wymuszania określonych dla grupy zasad bezpieczeństwa.
6	Oprogramowanie musi mieć możliwość konfiguracji rozwiązania, które będzie dla wyznaczonych agentów punktem dystrybuującym uaktualnienia i poprawki oprogramowania.
7	W obrębie jednej konsoli zarządzającej system musi pozwalać na kontrolę integralności hypervisora środowiska wirtualnego.
8	Oprogramowanie musi umożliwiać zdefiniowanie harmonogramu lub częstotliwości pobierania aktualizacji wirusów od producenta systemu.
9	Oprogramowanie musi wykorzystywać mechanizmy cache i deduplikacji w celu optymalizacji czasu skanowania i wykrywania zmian.
10	Oprogramowanie musi umożliwiać instalację i konfigurację lokalnego serwera skorelowanej reputacji plików, adresów e-mail oraz adresów URL, synchronizującego się z chmurą producenta, który pozwalał będzie na weryfikację reputacji plików i adresów URL bez konieczności łączenia się z Internetem.
11	Oprogramowanie musi pozwalać administratorowi na określenie reakcji w przypadku wykrycia wirusa.
12	Oprogramowanie musi pozwalać na określenie obszarów skanowania, tj.: pliki, katalogi, itd.
13	Oprogramowanie musi pozwalać na określenie typów skanowanych plików, momentu ich

	skanowania (otwarcie, modyfikacja) oraz na wykluczenie ze skanowania określonych folderów.
14	Rozwiązanie musi chronić przed złośliwym oprogramowaniem, systemy oparte na MS Windows, Linux (RHEL, SuSE) w czasie rzeczywistym.
15	Oprogramowanie musi pozwalać na zarządzanie zdarzeniami i natychmiastowe alarmowanie i raportowanie o aktywności wirusów w chronionej infrastrukturze.
16	Zarządzanie systemem musi odbywać się poprzez standardową przeglądarkę WWW i połączenie https, która nie wymaga instalacji żadnych dodatkowych komponentów.
17	Oprogramowanie musi posiadać możliwość powiadamiania o wszystkich zdarzeniach za pomocą poczty elektronicznej, wiadomości SNMP lub wywołania komendy.
18	Oprogramowanie musi umożliwiać tworzenie kont administratorów o różnych stopniach uprawnień w stosunku do różnych modułów i funkcjonalności systemu, a także w stosunku do różnych chronionych obiektów lub grup obiektów.
19	Zarządzanie rolami w systemie musi pozwalać na zdefiniowanie uprawnień dających możliwość administrowania wyłącznie jednym chronionym obiektem oraz pojedynczymi funkcjonalnościami systemu bez możliwości zmiany nadrzędnego profilu bezpieczeństwa
20	Oprogramowanie musi pozwalać na tworzenie struktur zarządzanych komputerów również poprzez adresacje IP komputera który podlega zarządzaniu.
21	Oprogramowanie musi umożliwiać na jednoczesny dostęp do konsoli zarządzającej niezależnie przez kilku administratorów.
22	Oprogramowanie musi posiadać możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
23	Oprogramowanie nie może wymagać restartu chronionych komputerów i serwerów po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
24	Oprogramowanie musi pozwalać na wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan".
25	Oprogramowanie musi pozwalać na automatyczne usuwanie wirusów i zgłaszanie alertów w przypadku wykrycia wirusa.
26	Oprogramowanie musi zapewniać w procesie skanowania ręcznego i automatycznego przeskanowania dowolnego celu pod względem złośliwego oprogramowania.
27	Rozwiązanie powinno pozwalać na notyfikację (powiadomienie użytkownika) w przypadku skorzystania z niebezpiecznych zasobów lub pobrania niebezpiecznego pliku. Notyfikacja powinna dotyczyć pracy w trybie agentowym lub bezagentowym.
28	Oprogramowanie musi posiadać możliwość kontroli oraz blokowania aplikacji próbujących uzyskać połączenie z Internetem lub siecią lokalną.

29	Oprogramowanie musi posiadać możliwość heurystycznego wykrywania transmisji na podstawie częstotliwości jej występowania oraz zdefiniowanego zakresu portów.
30	Wszystkie funkcjonalności systemu muszą być zarządzane z jednej, centralnej konsoli.
31	W przypadku ochrony w trybie agentowym wszystkie funkcjonalności systemu muszą być dostępne w ramach pojedynczego agenta instalowanego na chronionych obiektach.
32	Oprogramowanie musi umożliwiać nanoszenie zmian w profilach bezpieczeństwa w czasie rzeczywistym bez potrzeby restartu systemu i chronionych obiektów.
33	Oprogramowanie musi umożliwiać tworzenie dowolnej ilości profili bezpieczeństwa zawierających predefiniowane reguły ochronne.
34	Oprogramowanie musi umożliwiać automatyzację aplikowania profili bezpieczeństwa poprzez zdefiniowanie filtra zawierającego nazwę, system operacyjny, serwer ESX czy instancję wykorzystującą chmurę.
35	Oprogramowanie musi umożliwiać automatyczną zmianę przypisanych profili bezpieczeństwa w przypadku zmiany IP przez chroniony system informatyczny.
36	Oprogramowanie musi umożliwiać generowanie na żądanie oraz wg. harmonogramu raportów w formatach minimalnie RTF oraz PDF oraz możliwość zabezpieczenia raportu poprzez jego zaszyfrowanie lub zabezpieczenie hasłem.

9.10 Oprogramowanie wykonywania kopii zapasowej środowiska wirtualizacji

Dostarczenie licencji na oprogramowanie do wykonywania kopii bezpieczeństwa posiadanego przez Zamawiającego środowiska wirtualizacji VMware vSphere Enterprise plus na 40 procesorów fizycznych hostów ESX.
Wszystkie licencje mają być dostarczone wraz ze wsparciem technicznym z czasem trwania wsparcia technicznego, zgodnym z ofertą Wykonawcy - „Czas Trwania Wsparcia Technicznego”, świadczonym przez producenta będącego licencjodawcą oprogramowania, które powinno umożliwiać zgłaszanie problemów 5 dni w tygodniu przez 12h na dobę oraz pobieranie i instalowanie nowych poprawek, wersji oprogramowania.

ID	Wymaganie
1	Oferowane licencje muszą zapewnić backup / odtwarzanie środowiska VMware składającego się z 20 serwerów ESX posiadających łącznie 40 fizycznych procesorów
2	System centralnego backupu musi umożliwiać dla powyżej definiowanego środowiska VMware backup/odtwarzanie nielimitowanej liczby maszyn wirtualnych: Zarówno backup obrazów maszyn wirtualnych jak również backup ze środka maszyn wirtualnych wszystkimi dostępnymi agentami oprogramowania backupowego

3	Wymaga się by w ramach oferowanych licencji system umożliwiał backup maszyn wirtualnych w każdym trybie: • Jako obrazy maszyn wirtualnych VMware(pliki vmdk) • Ze środka, agentem plikowym / bazodanowym / aplikacyjnym dla systemów plików Oracle, SQL, Sybase, DB2, Exchange, Lotus, Sharepoint Musi być możliwość backupu jak powyżej dla dowolnej liczby maszyn wirtualnych w ramach zaintonowanych serwerów ESX.
4	Serwer backupu musi być dostarczony do zainstalowania na 2 fizycznych serwerach zarządzających backupem i odtwarzaniem całości zabezpieczanego środowiska.
5	Oferowany system musi tworzyć centralny system backupu wykonujący kopie zapasowe oraz zapewniać przechowywanie wszystkich zdeduplikowanych kopii zapasowych na dyskach posiadanego prze Zamawiającego de-duplikatora.
6	Całość backupów musi być składowana na posiadanym przez Zamawiającego de-duplikatorze EMC DataDomain..
7	Oprogramowanie backupowe musi być wspierane (kompatybilne) z posiadanym przez Zamawiającego de-duplikatorem EMC DataDomain.
8	Każdy z serwerów backupu musi umożliwiać: • zarządzanie backupem lokalnego środowiska i związanych z nim zdalnych lokalizacji • przechowywanie backupów na dyskach posiadanego przez Zamawiającego de-duplikatora • zarządzanie replikacją między przez Zamawiającego de-duplikatorami • odtworzenie zreplikowanych backupów ze zdalnego urządzenia backupowego również w przypadku całkowitego zniszczenia zdalnego ośrodka czyli zniszczenia całości zdalnego środowiska backupu • stanowić kompletny system centralnego backupu z agentami do backupu plików, baz danych, środowisk wirtualnych.
9	Dostarczony system musi przechowywać kopie zapasowe na dyskach posiadanego przez Zamawiającego de-duplikatora EMC DataDomain.
10	Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) następujące systemy operacyjne: Windows (także Microsoft Cluster) , Linux (Red Hat, SUSE, Debian, CentOS, Ubnutu, Novell OES), FreeBSD.
11	Backup zasobów plików z powyższych systemów musi podlegać de-duplikacji ze zmiennym blokiem na zabezpieczanej maszynie zgodnie z wymaganiami w mniejszej specyfikacji.
12	Oprogramowanie backupowe musi umożliwiać backup całych obrazów maszyn wirtualnych systemu VMware.
13	Oprogramowanie backupowe musi w trakcie backupu przesyłać do posiadanego przez Zamawiającego de-duplikatora tylko unikalne bloki, czyli bloki nie znajdujące się na oferowanym de-duplikatorze skracając czas backupu, obciążenie procesora i zmniejszając ruch w sieci WAN / LAN.
14	Włączenie funkcjonalności deduplikacji nie może generować wymogu instalacji dodatkowych

	modułów programowych po stronie klienckiej lub serwera backupowego.
15	Oprogramowanie backupowe nie może odczytywać tych plików z systemu dyskowego, które się nie zmieniły w stosunku do ostatniego backupu. Raz zbackupowany plik nie może być nigdy więcej odczytany, chyba, że zmieni się jego zawartość.
16	W konsoli oprogramowania backupowego musi być możliwość definiowania ważności danych (backupów) na podstawie kryteriów czasowych (dni, miesiące, lata). Po okresie ważności backupy musza być automatycznie usunięte.
17	Oferowanie oprogramowanie backupowe musi mieć możliwość tworzenia z poziomu GUI (konsoli graficznej) polityk typu Dziadek – ojciec –syn, to znaczy utworzenia polityki w której zdefiniowano: • Czas przechowywania backupów dziennych, • Czas przechowywania backupów tygodniowych, • Czas przechowywania backupów miesięcznych, • Czas przechowywania backupów rocznych.
18	Oferowane rozwiązanie musi umożliwiać tworzenie wykluczeń, czyli elementów nie podlegających backupowi w ramach zadania backupowego. Musi istnieć możliwość tworzenia wykluczeń dla dowolnej kombinacji następujących elementów: • wybranych typów plików, • dla całych katalogów, • dla pojedynczych plików
19	Oferowane rozwiązanie musi mieć możliwość zdefiniowania by ostatni backup dowolnego zbioru danych nigdy się nie przeterminował. Oznacza to, że jeśli dany zasób nie jest backupowany to automatycznie ostatnie ważny backup tego zasobu jest trzymany bezterminowo. Jedynie administrator może zdecydować o jego usunięciu.
20	Serwery backupu muszą zarządzać replikacją backupów znajdujących się na de-duplikatorze. Całość konfiguracji replikacji backupów musi odbywać się z konsoli serwera backupu. Konfiguracja zadań replikacji nie może wymagać jakichkolwiek działań na de-duplikatorze.
21	Wymaga się by replikacja między backupów znajdujących się na de-duplikatorach odbywała się w obu kierunkach jednocześnie: • Backupy z de-duplikatora z ośrodka podstawowego do de-duplikatora z ośrodka zapasowego • Backupy z de-duplikatora z ośrodka zapasowego do de-duplikatora z ośrodka podstawowego Całość replikacji zarządzana tylko i wyłącznie z poziomu oprogramowania backupowego (serwerów backupu)

22	Musi istnieć możliwość zdefiniowania kalendarza replikacji między serwerami oraz zdefiniowania które zadania backupowe podlegają replikacji. Serwer backupu musi udostępniać (pokazywać w konsoli GUI) backupy które zostały do niego zreplikowane ze zdalnej lokalizacji. Musi być możliwość odtworzenia backupów zreplikowanych do lokalnego serwera backupu / de-duplikatora ze zdalnej lokalizacji. Odtworzenie musi dobywać się poprzez interfejs GUI. Odtworzenie musi być możliwe w przypadku całkowitej niedostępności zdalnego systemu backupu (nieodstępność zdalnego serwera backupu oraz zdalnego de-duplikatora). Każdy serwer backupu w każdej lokalizacji musi udostępniać (pokazywać w konsoli GUI) zarówno lokalne backupy jak wszystkie również backupy zreplikowane do ośrodka zdalnego. W przypadku odtwarzania danych w ośrodku A w trakcie definiowania zadania odtwarzania musi być możliwość zdefiniowania czy odtwarzamy backupy z lokalnej kopii (znajdujące się na lokalnym oferowanym de-duplikatorze) czy też odtwarzamy ze zdalnej kopii z ośrodka B (znajdujące się na zdalnym oferowanym de-duplikatorze w lokalizacji B). Konsola zarządzająca systemem backupowym musi integrować się z Active Directory. Musi być możliwość przydzielania użytkownikom i grupom Active Directory dostępnych ról (min, administrator, monitoring, tylko wykonywanie odtworzenia) w systemie backupowym. Konsola musi udostępniać raporty dotyczące zajętości przestrzeni przeznaczonej na deduplikaty. Oprogramowanie backupowe musi mieć możliwość limitowania wielkości zadania backupowego. Jeśli zadanie backupowe przekroczy zdefiniowaną wielkość wówczas nie może być zapisane w systemie backupowych Oprogramowanie backupowe musi umożliwiać ograniczenie mocy procesora używanej do wykonywania zdania backupu tak by odpowiednia moc procesora zostawić dla innych zadań.
23	Rozwiązanie backupowe musi wspierać backup i odtwarzanie środowisk VMware 6.0. Oprogramowanie backupowe musi umożliwiać dla środowisk VMware następujące typy backupu: a. Backup całych maszyn wirtualnych b. Backup pojedynczych, wybranych dysków maszyny wirtualnej vmdk c. W trakcie backupu odczytowi z systemu dyskowego mają podlegać tylko zmienione bloki wirtualnych maszyn systemu VMware (wymagane wykorzystanie mechanizmu CBT systemu VMware) d. Wszystkie backupy obrazów maszyn wirtualnych muszą być wykonywane przy pomocy technologii CBT systemu VMware to znaczy do medium backupowego z systemu VMware muszą być transferowane tylko zmienione bloki. Jednocześnie z punktu widzenia systemu backupowego musza to być backupy pełne (full backupy). To znaczy z punktu widzenia systemu backupu muszą to być backupy identyczne z wykonywanym od zera pełnym backupem. e. Musi istnieć możliwość zastosowania wyrażeń regularnych do określenia które wirtualne dyski VMware mają być backupowane. f. Wykonywanie backupu obrazów maszyn wirtualnych VMware nie może wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych (plików vmdk) Powyższe metody backupu maszyn wirtualnych muszą podlegać de-duplikacji ze zmiennym blokiem przed wysłaniem danych do medium backupowego zgodnie z wymaganiami dla de-duplikacji powyżej. Powyższe metody backupu muszą być wbudowane w system backupu i w pełni automatyczne

	bez wykorzystania skryptów/dodatkowych komend.
24	Oferowany system musi pozwalać na szybkie odtworzenie • całych obrazów maszyn wirtualnych • pojedynczych dysków maszyny wirtualnej z backupu całej maszyny wirtualnej
25	Rozwiązanie backupowe musi umożliwiać odtworzenie obrazów maszyn wirtualnych VMware dostarczając następujące funkcjonalności: a. Odtworzenie całych maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu. b. Odtworzenie pojedynczych dysków maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu. c. Odtworzenie pojedynczych plików z backupu obrazu maszyny wirtualnej bez konieczności odtworzenia całej maszyny wirtualnej. Funkcjonalność musi być dostępna dla obrazów maszyn wirtualnych z zainstalowanym systemem operacyjnym Windows oraz Linux. d. Możliwość zamontowania na dowolnym serwerze (fizycznym lub wirtualnym) zbackupowanych obrazów maszyn wirtualnych Windows (plików vmdk maszyny wirtualnej Windows). Powyższa metoda nie może fizycznie odtwarzać backupów a jedynie pozwalać na przeglądanie zawartości plików vmdk w backupie z poziomu Eksploratora Plików Windows na dowolnej maszynie. Powyższe metody odtworzenia muszą być wbudowane w system backupu i w pełni automatyczne bez wykorzystania skryptów/dodatkowych komend.
26	Rozwiązanie backupowe musi umożliwiać uruchomienie maszyny wirtualnej bezpośrednio z medium backupowego bez konieczności odtwarzania (Instant Access).
27	Oprogramowanie backupowe musi mieć możliwość prezentacji (bez konieczności odtworzenia) zbackupowanych obrazów maszyn wirtualnych VMware (plików vmdk) jako katalogów na maszynie fizycznej celem ich przeszukiwania (wymagane przeszukiwanie po nazwach plikó jak również zawartości plików) z poziomu systemu operacyjnego maszyny fizycznej.
28	Oprogramowanie backupowe musi mieć możliwość backupu / odtworzenia w trybie „image backup” (backup plików vmdk) maszyn wirtualnych znajdujących się na serwerach VMware ESX bez udziału vCenter.
29	Skalowalność rozwiązania dla środowisk VMware musi być na poziomie: • Minimum 3000 maszyn wirtualnych w ramach pojedynczej instancji systemu backupu. • Minimum 100 maszyn wirtualnych backupowanych w ciągu godziny w ramach pojedynczej instancji systemu backupu.
30	Rozwiązanie backupowe musi umożliwiać backup i odtwarzanie w tym samym czasie minimum 50 maszyn wirtualnych VMware.

31	Oprogramowanie backupowe musi mieć możliwość automatycznego sprawdzania (weryfikacji) zbackupowanych maszyn wirtualnych VMware. Musi istnieć możliwość ustawienia kalendarza weryfikacji maszyn wirtualnych VMware. Weryfikacja maszyn wirtualnych musi zapewniać minimum: a. Odtworzenie maszyny wirtualnej na zdefiniowanym Data Center / Data Store, b. Weryfikacja podstawowych procesów, c. Możliwość dołączenia własnego skryptu weryfikującego wybrane elementy maszyny wirtualnej. Informacja w konsoli systemu backupu o poprawnej / niepoprawnej weryfikacji maszyny wirtualnej.
32	Administrator (właściciel) danej maszyny wirtualnej VMware musi mieć możliwość samodzielnego (bez konieczności kontaktu z administratorem backupu czy tez administratorem VMware) odtworzenia pojedynczych plików z dowolnego backupu obrazu jego maszyny wirtualnej.
33	Oprogramowanie backupowe musi zawsze przechowywać pełne backupy obrazów maszyn wirtualnych środowiska VMware/HyperV dla każdej wykonanej w przeszłości kopii zapasowej. Każdy backup obrazu maszyny wirtualnej musi być backupem pełnym.
34	Rozwiązanie backupowe musi pozwalać automatyczne polityki backupowe dla: • Folderu, • Resource Pool systemu VMware. Oznacza to, że dodanie maszyny wirtualnej do folderu, hosta czy resource pooli w systemie VMware spowoduje automatyczne backupowanie dodanej maszyny wirtualnej zgodnie z polityka zdefiniowana dla folderu hosta czy resource pooli w systemie VMware.
35	Rozwiązanie backupowe musi umożliwiać zdefiniowanie polityk backupowych dostępnych dla administratora systemu VMware z poziomu vCenter. Administrator VMware musi mieć możliwość przyporządkowania nowo tworzonych maszyn wirtualnych do polityk backupowych.
36	Oferowany system musi automatycznie naprawiać problemy związane ze snapshotami VMware. W przypadku gdy system VMware nie usunie snapshotu, oprogramowanie backupowe musi automatycznie ponawiać usunięcie snapshotu a w przypadku konieczności automatycznie konsolidować maszyny wirtualne VMware.
37	Backup oraz odtworzenie maszyn wirtualnych VMware musi być możliwy z poziomu graficznego interfejsu, linii komend oraz przez REST API.
38	Musi istnieć możliwość odtworzenia danych: • z zabezpieczanego serwera / komputera, • z konsoli systemu backupowego.
39	System backupu musi mieć funkcjonalność wyrzutu na taśmę.
40	Opcja wyrzutu na taśmę musi być elementem niniejszej oferty.
41	System backupu musi mieć możliwość bezpośredniego raportowania o błędach do serwisu producenta.

42	System backupu musi mieć możliwość instalacji agentów jako plików msi. Musi istnieć możliwość automatyzacji agentów poprzez uruchomienie skryptu instalującego agenta na zabezpieczanej maszynie i przyporządkowującego maszynę automatycznie do określonej polityki backupowej.
43	System backupu musi mieć możliwość automatycznej samo-aktualizacji poprzez automatyczne ściąganie nowych wersji od producenta.
44	System backupu musi mieć możliwość automatycznej aktualizacji oprogramowania agentów wykonywanej bezpośrednio z serwera backupu.
45	W ramach licencji musi być zapewniona możliwość monitorowania, raportowania.

9.11 Oprogramowanie ITSM

Wszystkie licencje mają być dostarczone wraz z wsparciem technicznym, z czasem trwania wsparcia technicznego, zgodnym z ofertą Wykonawcy - „Czas Trwania Wsparcia Technicznego", świadczonym przez producenta będącego licencjodawcą oprogramowania, które powinno umożliwiać zgłaszanie problemów oraz pobieranie i instalowanie nowych poprawek, wersji oprogramowania.

1. Oprogramowanie musi posiadać następujące elementy składowe:

ID	Wymaganie
1.	Moduł procesów umożliwiający zarządzanie co najmniej wymienionymi procesami w rozumieniu biblioteki ITIL: I. Zarządzanie incydentem, II. Zarządzanie problemem, III. Zarządzanie zmianą, IV. Zarządzanie konfiguracją, V. Zarządzanie projektami, VI. Zarządzanie wnioskiem o usługę.
2.	Centralną bazę konfiguracji CMDB wraz ze zintegrowanym wykrywaniem środowiska IT.
3.	Moduł zarządzania umowami serwisowymi dla elementów konfiguracji (CI) przechowywanych w bazie konfiguracji CMDB.
4.	Moduł zarządzania bazą wiedzy dla użytkowników.
5.	Moduł raportowania.

2. Wymagania ogólne

ID	Wymaganie
1.	Oprogramowanie musi pochodzić z Polskiego oficjalnego kanału dystrybucji,
2.	Oprogramowanie musi być objęte wsparciem technicznym realizowanym w języku polskim przed podmiot autoryzowany do świadczenia tej usługi przez producenta oprogramowania,
3.	Oprogramowanie musi umożliwiać utworzenie i jednoczesną pracę (konta nazwane) do 100 techników oraz przechowywanie informacji do min. 15000 elementów konfiguracji w bazie konfiguracji z czego min. 2500 elementów musi podlegać wykrywaniu przez moduł CMDB,
4.	Oprogramowanie pozwala na reprezentacje użytkowników z wykorzystaniem imienia i nazwiska użytkownika,
5.	Oprogramowanie umożliwia odwzorowanie wielodziałowej struktury organizacyjnej przedsiębiorstwa, gdzie dla każdego oddziału możliwe będzie zdefiniowanie zespołu techników, użytkowników, grup wsparcia, reguł automatycznego przypisywania zgłoszeń, czasów rozwiązywania zgłoszeń, dni wolnych i godzin pracy,
6.	Interfejs oprogramowania jest w całości dostępny w języku polskim, wraz z możliwością wprowadzania zmian w słownikach atrybutów konfiguracji oraz słowników interfejsu graficznego użytkownika,
7.	Dostęp do oprogramowania, w tym pełna konfiguracja systemu jest możliwa poprzez interfejs WEB aplikacji,
8.	Oprogramowanie musi umożliwiać realizację połączeń z aplikacją poprzez bezpieczny kanał komunikacji, operaty na protokole https i certyfikatach kwalifikowanych lub innym równoważnym rozwiązaniu,
9.	Oprogramowanie umożliwia integrację użytkowników aplikacji z domeną Active Directory lub katalogiem LDAP,
10.	Integracja aplikacji z domena Active Directory pozwala na import dowolnego atrybutu UDF z AD oraz na wykorzystanie mechanizmu SSO dla użytkowników,
11.	Oprogramowanie serwera musi pracować na systemie operacyjnym Microsoft Windows w wersji 32 lub 64 bitowej lub Linux Debian w wersji 32 bitowej lub 64 bitowej, lub Linux RedHat w wersji 32 bitowej lub 64 bitowej oraz współpracować przynajmniej z jedną z baz danych: MySQL, Microsoft SQL lub POSTGRESQL.
12.	System musi posiadać możliwość skonfigurowania architektury HA, funkcjonalność musi być częścią dostarczonego systemu.

3. Wymagane funkcjonalności dla poszczególnych modułów wchodzących w skład oprogramowania

ID	Wymaganie
I	**Moduł zarządzania procesami**

1.	Moduł zarządzania procesami musi być w pełni konfigurowalny z poziomu interfejsu webowego oprogramowania,
2.	Dostęp do modułu zarządzania procesami odbywa się z poziomu przeglądarki internetowej zarówno dla serwisanta jak i użytkownika systemu,
3.	System musi posiadać możliwość dostosowania portalu w tym, rozmieszczenie poszczególnych elementów portalu metodą drag&drop, zagnieżdżanie stron html,
4.	System musi posiadać mechanizm oznaczania pierwszej reakcji na zgłoszenie, jako rozwiązania zgłoszenia – first call resolution,
5.	System musi posiadać możliwość oznaczenia pracy nad zgłoszeniem przez danego serwisanta, oznaczenie pracy uruchamia zegar naliczający czas pracy serwisanta nad zgłoszeniem. System w postaci graficznej prezentuje uruchomiony zegar w widoku zgłoszeń, jak i samym zgłoszeniu,
6.	System pozwala określić typ czasu pracy poświęconego na rozwiązanie zgłoszenia,
7.	System pozwala na dowolną rozbudowę pól wykorzystywanych do opisania czasu pracy poświęconego na rozwiązanie zgłoszenia,
8.	Moduł zarządzania procesami umożliwia rejestrację zgłoszenia wieloma kanałami, w szczególności przez stronę WWW, telefon i email,
9.	System posiada możliwość przekazywania wiadomości od serwisanta, bezpośrednio na skrzynkę pocztową zgłaszającego,
10.	Moduł zarządzania procesami umożliwia w trakcie rejestracji zgłoszenia przez użytkownika na stronie www załączenia dowolnego formatu załączników,
11.	Moduł zarządzania incydentami pozwala wstrzymać zegar SLA zgłoszenia wraz z ustawieniem automatycznego jego otwarcia i wysłania powiadomienia do serwisanta,
12.	Moduł zarządzania procesami umożliwia użytkownikom przeglądanie na stronie www statusu własnych zgłoszeń, dodawania komentarzy, podgląd i edycję danych użytkownika, prowadzenie projektów oraz przeglądania bazy wiedzy znanych problemów i ich rozwiązań,
13.	Moduł zarządzania procesami umożliwia definiowanie dodatkowych pól w formularzu incydentu, wniosku o usługę, problemu, zmiany,
14.	Moduł zarządzania zgłoszeniami (0bsługa zgłoszeń incydentów i wniosków o usługę) zapewnia budowę dynamicznych szablonów zgłoszeń. Dynamiczność szablonu zgłoszeń polega na automatycznym i samodzielnym dostosowaniu się szablonu zgłoszenia, do wprowadzanych atrybutów przez użytkownika. System pozwala na: • Uruchamianie i wyłączanie z zgłoszenia wskazanych atrybutów, • Chowanie i odsłanianie wybranych atrybutów, • Oznaczanie i odznaczanie obligatoryjnych do wypełnienia atrybutów, • Uruchamianie skryptów, pisanych w wbudowanym w aplikację edytorze skryptów, • Uruchamianie powyższych automatyzacji na różnych etapach rejestrowania zgłoszenia, oraz od wprowadzanych bieżących atrybutów w zgłoszeniu;

15.	Moduł zarządzania zgłoszeniami pozwala na konfigurację dedykowanych do wybranych typów zgłoszeń incydentów i wniosków o usługę przycisków, wyzwalających następujące akcje: • Uruchomienie dedykowanego pliku html, powiązanego z wykonywalnym skryptem lub klasą na systemie helpdeskowym, • Uruchomienie dedykowanego pliku html, powiązanego z wykonywalnym skryptem lub klasą na systemie zintegrowanym z helpdeskowym, • Uruchomienie wykonywalnego skryptu lub klasy na systemie helpdeskowym, • Uruchomienie wykonywalnego skryptu lub klasy na systemie zintegrowanym z helpdeskowym,
16.	Moduł zarządzania zgłoszeniami pozwala na konfigurację globalnych reguł biznesowych, wywołujących wykonywalny skrypt lub klasę na systemie helpdeskowym, lub na systemie zintegrowanym z systemem helpdeskowym,
17.	Moduł zarządzania zgłoszeniami posiada możliwość wymuszenia podawania komentarzy przy zmianie statusów zgłoszenia,
18.	Moduł zarządzania zgłoszeniami posiada możliwość budowania zależności miedzy zarejestrowanymi zgłoszeniami incydentów i wniosków o usługę. Zależności muszą pozwalać na uzależnienie zamykania zgłoszenia od zamknięcia zgłoszenia zależnego poprzedzającego dane zgłoszenie,
19.	System pozwala na konfigurację funkcjonalności informującej zgłaszających o czasie na rozwiązanie zgłoszenia, dotyczy zarówno zgłoszeń incydentów jak i wniosków o usługę,
20.	Moduł zarządzania procesami posiada centralne repozytorium incydentów, wniosków o usługę, problemów i zmian, umożliwiające filtrowanie i sortowania zapisanych zgłoszeń według co najmniej następujących kryteriów: status zgłoszenia, kategoria, użytkownik, czas rozwiązania, czas przyjęcia, przydzielona grupa wsparcia,
21.	Moduł zarządzania procesami umożliwia centralne repozytorium incydentów, wniosków o usługę, problemów i zmian, umożliwiające definiowanie własnych filtrów umożliwiających sortowania zapisanych zgłoszeń,
22.	Moduł zarządzania incydentami jest certyfikowany przez fundację Pink Elephant,
23.	Moduł zarządzania procesami umożliwia dla każdego zgłoszenia określenie takich atrybutów, jak: dane osoby zgłaszającej, zasób, którego dotyczy zgłoszenie oraz priorytet, wpływ i pilność realizacji,
24.	Moduł zarządzania procesami umożliwia przeszukiwanie zgłoszeń według co najmniej następujących atrybutów: nr zgłoszenia, użytkownik, tytuł, opis, data utworzenia,
25.	Moduł zarządzania procesami umożliwia rejestrację zgłoszeń pochodzących z zewnętrznych narzędzi monitorujących, jednocześnie umożliwiając ich klasyfikację i na tej podstawie automatyczne przekazywanie do grup wsparcia,

26.	Moduł zarządzani procesami umożliwia przesyłanie i prezentowanie na stronie www powiadomień dla użytkowników i/lub serwisantów, przesyłanie powiadomień do pojedynczych użytkowników lub grup użytkowników/serwisantów,
27.	Moduł zarządzania procesami w ramach rozwiązywania zgłoszeń umożliwia komunikację z użytkownikiem poprzez pocztę elektroniczną i rejestrację wiadomości do właściwych wątków zgłoszeń,
28.	Moduł zarządzania procesami umożliwia klasyfikację zgłoszeń, problemu lub zmiany, w co najmniej 3 poziomowej strukturze drzewiastej, przy czym struktura klasyfikacji powinna być dowolnie edytowalna przez uprawnionych administratorów z poziomu interfejsu webowego systemu,
29.	Moduł zarządzania procesami umożliwia automatyczne wyliczenie i przydzielenie priorytetu do zgłoszenia na podstawie wprowadzonych do formularza zgłoszenia informacji o wpływie i pilności realizacji,
30.	Moduł zarządzania procesami pozwala na automatyczną eskalację zgłoszeń do grup wsparcia, na podstawie co najmniej następujących atrybutów: użytkownik, priorytet, poziom, wpływ, pilność, tytuł zgłoszenia, słowo kluczowe w tytule i treści zgłoszenia,
31.	Moduł zarządzania procesami umożliwia przekierowanie zgłoszeń do innych serwisantów lub grup wsparcia celem dalszej obsługi,
32.	Moduł umożliwia zmianę typu zgłoszenia z incydentu na wniosek o usługę wraz ze zmianą parametrów zgłoszenia i trybu jego realizacji, zgodnie z procedurą określoną dla właściwego typu wniosku,
33.	Moduł zarządzania procesami umożliwia tworzenie szablonów zgłoszeń z predefiniowanymi atrybutami i regułami przekazywania do odpowiednich zespołów wsparcia,
34.	Moduł zarządzania procesami umożliwia tworzenie harmonogramów dla zgłoszeń okresowych, a w ramach realizacji takiego zgłoszenia automatyczne przydzielanie zadań do serwisantów,
35.	Moduł zarządzania procesami umożliwia rejestrację historii incydentów, wniosków o usługę, problemów i zmian, zablokowaną do edycji dla użytkownika oprogramowania,
36.	Moduł zarządzania procesami umożliwia rejestrowanie aktywności i zleceń pracy związanych z poszczególnymi incydentami, wnioskami o usługę, problemami i zmianami oraz śledzenie czasu pracy nad zgłoszeniem,
37.	Moduł zarządzania procesami umożliwia rejestrowanie czasu pracy nad danym zgłoszeniem, problemem i zmianą przez poszczególnych serwisantów pracujących nad zgłoszeniem,
38.	Moduł zarządzania procesami umożliwia wstawianie plików graficznych w treści rozwiązania zgłoszenia,
39.	Moduł zarządzania procesami umożliwia globalne definiowanie szablonów wiadomości e-mail wykorzystywanych przez system do powiadamiania użytkowników o różnych zdarzeniach w

	systemie. Definiowanie szablonów odbywa się z poziomu interfejsu webowego aplikacji i umożliwiać zdefiniowanie treści powiadomienia, reguły wywołującej przesłanie powiadomienia oraz odbiorcy,
40.	Moduł zarządzania zgłoszeniami umożliwia definiowanie i filtrowanie szablonów zgłoszeń dedykowanych dla określonych grup użytkowników,
41.	Moduł zarządzania procesami umożliwia przesyłanie do użytkowników powiadomień o następujących zdarzeniach zarejestrowanych przez system: przyjęcie zgłoszenia, aktualizacja zgłoszenia, rozwiązanie zgłoszenia, zamknięcie zgłoszenia,
42.	Moduł zarządzania procesami ma wbudowaną funkcjonalność prezentowania w postaci graficznej istotnych wskaźników wydajności pozwalające na monitorowanie statusu poszczególnych procesów, moduł wskaźników pozwala ustalić okres odświeżania danych na tablicy wskaźników,
43.	Moduł zarządzania procesami umożliwia automatyczne zamykanie rozwiązanych zgłoszeń po określonym czasie,
44.	Moduł zarządzania procesami umożliwia przekazywanie do akceptacji osób trzecich działań podejmowanych w ramach rozwiązania zgłoszenia, np. akceptacja realizacji zlecenia na usługę serwisową,
45.	Moduł zarządzania procesami umożliwia wielostopniowy poziom akceptacji wniosków o usługę wraz zdefiniowaniem procesu powiadomień kierowanych do osób akceptujących,
46.	Moduł zarządzania procesami umożliwia przeglądanie bazy wiedzy z poziomu incydentu lub problemu i podłączanie rozwiązania z bazy rozwiązań do rozwiązania w zgłoszeniu,
47.	Moduł zarządzania procesami umożliwia implementację warunków umów SLA i na tej podstawie obliczania czasu rozwiązania incydentu lub wniosku o usługę. Atrybuty umowy SLA, na postawie których system wylicza czas rozwiązania incydentu lub wniosku o usługę muszą zawierać co najmniej taki parametr jak nazwa użytkownika, oddział, komputer, priorytet, pilność, wpływ, poziom,
48.	Moduł zarządzania wnioskami o usługi, musi posiadać możliwość zdefiniowania reguł biznesowych, z ich rozróżnieniem względem lokalizacji,
49.	Moduł zarządzania wnioskami o usługi, posiada możliwość zdefiniowania umów SLA, z ich rozróżnieniem względem lokalizacji,
50.	Moduł zarządzania procesami posiada wbudowaną funkcjonalność ankietowania użytkowników. Ankiety są rozsyłane przez aplikację automatycznie po zamknięciu incydentu,
51.	Moduł zarządzania procesami umożliwia automatyczną konwersję incydentu na problem oraz przyłączania wielu incydentów do jednego problemu,
52.	Moduł zarządzania problemami umożliwia zamknięcie powiązanych problemem incydentów

	w momencie zamykania problemu,
53.	Moduł zarządzania procesami umożliwia zarejestrowanie znanego błędu oraz rozwiązania niezależnie i prezentacji rozwiązania tymczasowego użytkownikom,
54.	Moduł zarządzania procesami umożliwia rejestrację i klasyfikację zmian, automatyczną konwersję problemu na zmianę oraz przyłączanie wielu incydentów i problemów do zmiany,
55.	Moduł zarządzania procesami umożliwia zarejestrowanie szczegółowych planów w zmianie, planu wdrożenia zmiany oraz planu wycofania zmiany,
56.	Moduł zarządzania procesami umożliwia połączenie zmiany z zasobami i usługami, których ta zmiana dotyczy,
57.	Moduł zarządzania procesami umożliwia przeprowadzenie procesu akceptacji dla zmiany przez komisję ds. zmiany (ang. Change Advisory Board),
58.	Moduł zarządzania procesami musi umożliwiać zdefiniowanie na formularzach incydentu, wniosku o usługę, problemu i zmiany pól niezbędnych do wypełnienia w trakcie rejestracji i zamknięcia zgłoszenia,
59.	Moduł zarządzania czasem pracy pozwala na rejestrację czasu pracy, przez uruchomienie zegara liczącego, czas spędzony nad zgłoszeniem przez technika,
60.	Moduł zarządzania czasem pracy, pozwala na analizę czasów: przypisania zgłoszenia do danego technika, przypisania zgłoszenia do danej grupy suportu, przypisania zgłoszenia do danego statusu,
61.	Moduł zarządzania czasem pracy pozwala na wprowadzanie dodatkowych atrybutów czasu pracy, możliwych do raportowania,
62.	Moduł zarządzania czasem pracy pozwala na wprowadzenie dedykowanych typów czasu pracy,
63.	Moduł zarządzania procesami umożliwia zdefiniowanie i zarządzanie projektami,
64.	Moduł zarządzania procesami umożliwia w ramach zdefiniowanego projektu określenie tzw. kamieni milowych projektu, osób zaangażowanych w projekt oraz przydzielenie im zadań na każdym etapie realizacji projektu,
65.	Moduł zarządzania procesami umożliwia definiowanie typów oraz statusów dla projektów wraz z możliwością filtrowania po tych parametrach,
66.	Moduł zarządzania procesami umożliwia definiowanie ról w projekcie i przypisywanie ich zaangażowanym osobom,
67.	Moduł zarządzania procesami pozwala na eksport widoku diagramu Gantta do pliku PDF,
68.	Moduł zarządzania procesami umożliwia przedstawienie w sposób graficzny zaawansowania realizacji poszczególnych etapów w projekcie,

69.	Moduł zarządzania zgłoszeniami jest udostępniony w aplikacjach mobilnych na systemach Android, zarówno dla kont serwisantów jak i zgłaszających.
II	**Centralna baza konfiguracji CMDB wraz ze zintegrowanym wykrywaniem środowiska**
1.	CMDB umożliwia przechowywanie danych o wszystkich jednostki konfiguracji (CI) takich jak: • Komputery, • Drukarki sieciowe, • Urządzenia sieciowe, • Pakiety oprogramowania, • Komponenty komputerów i urządzeń sieciowych, • Usługi biznesowe oraz IT, • Zasoby ludzkie (np. użytkownicy, grupy użytkowników, serwisanci, grupy serwisowe);
2.	CMDB zawiera gotowy schemat danych wraz z listą możliwych relacji pomiędzy jednostkami konfiguracji, jak również możliwość rozbudowanie go o własne, zdefiniowane relacje,
3.	CMDB umożliwia dynamiczne rozszerzenie schematu danych o dodatkowe atrybuty, w tym atrybuty dedykowane dla konkretnego typu jednostki konfiguracji CI. Rozszerzenie odbywa się z poziomu interfejsu graficznego systemu,
4.	CMDM umożliwia przedstawienie w sposób graficzny wzajemnych relacji pomiędzy jednostki konfiguracji CI,
5.	CMDB umożliwia przechowywanie informacji pomiędzy incydentami, problemami oraz zmianami, a jednostkami konfiguracji,
6.	CMDB umożliwia ręczne dodawanie jednostek konfiguracji oraz relacji pomiędzy nimi z poziomu interfejsu graficznego jak również importu danych o jednostkach konfiguracji z plików w formacie CSV lub XML,
7.	CMDB posiada zintegrowany moduł wykrywania środowiska IT, pozwalający na wykrycie co najmniej konfiguracji komputerów, serwerów i oprogramowania. Wykrywanie opiera się na połączeniach protokołem SSH oraz protokołami SNMP lub WMI lub również przy wykorzystaniu skanowania agendowego. System zapewnia opcjonalność wykorzystywanej metody skanowania środowiska IT,
8.	Moduł wykrywania środowiska umożliwia zbieranie danych o konfiguracji komputerów, co najmniej: • Ilości i rodzaju procesora, • Wielkość dostępnej pamięci fizycznej i wirtualnej , • Nr seryjny komputera, • Nazwa i wersja systemu operacyjnego, • Zainstalowane oprogramowanie i poprawki;
9.	Moduł wykrywania środowiska powinien posiadać mechanizm generowania kodów kreskowych dla zasobów. Moduł powinien pozwalać na zdefiniowanie formatu kodu kreskowego i jego

	wydruk według zdefiniowanego formatu wydruku,
10.	Moduł wykrywania zasobów powinien posiadać możliwość wprowadzania zasobów skanowanych po kodzie kreskowym,
11.	Moduł wykrywania środowiska umożliwia przeprowadzenie wykrywania zmian w konfiguracji i generowania raportów porównawczych zmian w elementach konfiguracji,
12.	Moduł wykrywania środowiska umożliwia przeprowadzenie automatycznych, zdefiniowanych według cyklicznego harmonogramu audytów konfiguracji komputerów i serwerów, pod kątem zmian w konfiguracji i zainstalowanym oprogramowaniu,
13.	Moduł wykrywania środowiska umożliwia przeprowadzenie skanowania komputerów i zasilenie danych do bazy dla komputerów niepodłączonych do sieci komputerowej. Możliwe jest zastosowanie specjalnych skryptów, których plik wynikowy następnie zostanie zaimportowany do bazy,
14.	CMDB umożliwia przechowywanie informacji o poszczególnych elementach konfiguracji w taki sposób, by możliwe było rejestrowanie i śledzenie historii posiadania elementu konfiguracji przez użytkowników, powiązanie z nim informacji o koszcie zakupu, innych kosztach eksploatacyjnych, warunkach umowy serwisowej, dostawcy,
15.	CMDB umożliwia wyszukiwanie elementów konfiguracji po dowolnych atrybutach, zarówno standardowych, jak i dodanych przez użytkownika, w tym po kodach kreskowych,
16.	CMDB umożliwia zdefiniowanie wartości początkową elementu konfiguracji oraz mierzenie jego amortyzacji,
17.	CMDB umożliwia powiązanie poszczególnych elementów konfiguracji z danymi użytkownika (jego imieniem i nazwiskiem, nr telefonu, departamentem), departamentu, innymi elementami konfiguracji i katalogiem usług,
18.	CMDB umożliwia przechowywanie informacji o posiadanych przez użytkownika licencjach na oprogramowanie, powiązać posiadane licencje z zainstalowanym na komputerach oprogramowaniem, oraz rejestrować historię zmian posiadania danej licencji,
19.	CMDB umożliwia zarządzanie licencjami na oprogramowanie posiadane przez użytkowników w tym zarządzanie umowami dotyczącymi zakupu licencji oraz zasilanie CMDB danymi dotyczącymi licencji pochodzącymi z innych źródeł danych,
20.	CMDB umożliwia wygenerowanie raportu posiadanych licencji przez użytkownika oraz raportów zgodności licencji z zainstalowanym oprogramowaniem,
21.	CMDB umożliwia z poziomu interfejsu oprogramowania nawiązanie sesji zdalnej w trybie przejęcia pulpitu użytkownika z komputerem przechowywanym w bazie,
22.	CMDB posiada API,
III	**Moduł zarządzania umowami serwisowymi dla zasobów IT przechowywanych w bazie**

	konfiguracji CMDB:
1.	Moduł zarządzania umowami serwisowymi umożliwia rejestrację warunków umów gwarancyjnych i serwisowych, w tym w szczególności dane teleadresowe gwaranta, czas obowiązywania umowy, jej koszt oraz powiązania ich z jednym lub wieloma elementami konfiguracji bazy CMDB,
2.	Moduł zarządzania umowami serwisowymi posiada funkcjonalność pozwalającą przesyłać powiadomienia o wygaśnięciu okresu obowiązywania umowy serwisowej i gwarancyjnej;
IV	**Moduł zarządzania bazą wiedzy dla użytkowników**
1.	Moduł zarządzania bazą wiedzy umożliwia rejestrację rozwiązań zawierających co najmniej następujące atrybuty: temat i opis rozwiązania, powiązane słowa kluczowe, klasyfikacja rozwiązania,
2.	Moduł zarządzania bazą wiedzy umożliwia klasyfikację rozwiązań w strukturze drzewiastej katalogu, dowolnie definiowanego przez użytkownika,
3.	Moduł zarządzania bazą wiedzy umożliwia przeszukiwanie danych po dowolnych atrybutach rozwiązania,
4.	Moduł zarządzania bazą wiedzy umożliwia udostępnianie rozwiązań osobno dla użytkowników i osobno dla serwisantów,
5.	Moduł zarządzania bazą wiedzy umożliwia rejestrację rozwiązań z poziomu incydentu i problemu,
6.	Moduł zarządzania bazą wiedzy umożliwia przeglądanie rozwiązań bez konieczności logowania się użytkownika do systemu,
7.	Moduł bazy wiedzy umożliwia dokonanie akceptacji dodawanego do bazy wiedzy rozwiązania przez administratora bazy wiedzy,
8.	Moduł zarządzania bazą wiedzy umożliwia zamieszczanie i wyświetlanie w treści rozwiązania plików graficznych oraz dołączania dowolnej ilość załączników,
9.	Moduł zarządzania bazą wiedzy umożliwia przesłanie rozwiązania do użytkownika za pomocą poczty elektronicznej bez konieczności powiązania tego działania z procesem zarządzania incydentem lub problemem,
10.	Moduł Bazy wiedzy może być ukryty przed zgłaszającymi,
11.	Moduł Bazy Wiedzy posiada API;
V	**Moduł zarządzania zakupami**
1.	Moduł zarządzania zakupami umożliwia przeprowadzenie procesu zakupowego składającego się z co najmniej następujących kroków: • Utworzenie zamówienie – rejestracja numeru zamówienia, powiązanie z dostawcą, określenie terminu realizacji zamówienia,

	• Dodanie pozycji do zamówienia – rejestracja produktów, ich ilości oraz ceny jednostkowej produktu, • Przedstawienie zamówienia do akceptacji – moduł zarządzania zakupami umożliwia przeprowadzenie weryfikacji i akceptacji zamówienia przez osoby trzecie, z tymże użytkownik rejestrujący zamówienie nie może być jednocześnie osobą trzecią weryfikującą i akceptującą realizację zamówienia, • Powiązanie zamówienia z elementami konfiguracji w bazie CMDB;
2.	Moduł zarządzania zakupami umożliwia przesłanie powiadomienia do osób trzecich o przekroczonym terminie realizacji zamówienia,
3.	Moduł zarządzania zakupami umożliwia przydzielenie zamówienia do wybranego centrum kosztów (Cost Center) oraz konta księgi głównej w księgowości.
VI	**Moduł raportowania**
1.	Moduł raportowania umożliwia utworzenie raportów zarejestrowanych incydentów, problemów i zmian filtrowanych według kategorii, departamentu, statusu zgłoszenia, użytkownika,
2.	Moduł raportowania umożliwia utworzenie raportów przedstawiających rozkład incydentów w czasie według dowolnego atrybutu, próbkowane co jeden dzień roboczy,
3.	Moduł raportowania umożliwia utworzenie raportów czasu pracy użytkowników w ramach rozwiązywania zgłoszeń,
4.	Moduł raportowania posiada wbudowaną funkcjonalność exportu utworzonych raportów do plików formatu PDF, XLS i HTML,
5.	Moduł raportowania umożliwia automatyczne tworzenie raportów, zdefiniowanych według cyklicznego harmonogramu a następnie przesyłanie tychże raportów za pomocą poczty elektronicznej do dowolnego użytkownika,
6.	Moduł raportowania umożliwia dostęp do modułu tylko wybranym użytkownikom,
7.	Moduł raportowania jest wyposażony w funkcjonalność wykonywania zapytań SQL do bazy danych oprogramowania, funkcjonalność ta jest realizowana poprzez interfejs webowy oprogramowania,
8.	Moduł raportowania pozwala na tworzenie dynamicznych wskaźników. Prezentowanych w tablicy wskaźników,
9.	Moduł raportowania umożliwia przyłączenie do niego zewnętrznych systemów raportujących, takich jak Crystal Reports lub równoważnych.

9.12 Urządzenia sieciowe

Dla następujących urządzeń sieciowych: Przełącznik Data Center LAN typu SPINE, Przełącznik Data Center LAN typu LEAF, Router BGP, Przełącznik LAN typu Top of the Rack, Przełącznik Koncentrujący Top of the Rack, Firewall Data Center; należy dostarczyć oprogramowanie do centralnego zarządzania wymienionymi urządzeniami.

9.12.1 Przełączniki Data Center LAN typu SPINE – 2 szt.

Produkt musi spełnić następujące wymagania:

ID	Wymagania dla przełączników Data Center LAN typu SPINE - 2 sztuki
1.	Wymagana architektura sieci LAN musi być oparta o architekturę typu SPINE-LEAF, z podziałem ról przełączników, tworzących tzw. IP Fabric. Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do montowania w szafie rack 19''.
2.	Producent powinien oferować wsparcie dla modułów optycznych realizujących transmisję pochodzących od innych niż producent urządzeń dostawców.
3.	Przełącznik typu SPINE musi być wyposażony w co najmniej 32 porty 40GbE w konfiguracji: 24 wbudowane porty oraz łącznie 8 w modułach rozbudowy, wraz z zainstalowanymi 32 wkładkami QSFP+. Maksymalna długość kabli połączeniowych nie przekroczy 150m.
4.	Przedstawione rozwiązanie powinno zawierać: - 2 szt. przełącznik typu SPINE oferowane urządzenia muszą zapewnić rozbudowę do co najmniej: - 4 szt. przełącznik SPINE
5.	Przełącznik musi posiadać wymienny zasilacz AC. Przełącznik musi być wyposażony w dodatkowy redundantny zasilacz. Musi posiadać możliwość wymiany wszystkich modułów na gorąco (hot swap). Przełączniki musza wspierać funkcjonalność ISSU.
6.	Przełącznik musi być wyposażony w port konsoli oraz dedykowany interfejs Ethernet do zarządzania OOB (out-of-band).
7.	Przełącznik musi być wyposażony w nie mniej niż 2 GB pamięci Flash oraz 2 GB pamięci DRAM. Ilość zainstalowanej pamięci RAM powinna zapewniać prawidłową pracę urządzenia oraz oprogramowania.
8.	Zarządzanie urządzeniem musi odbywać się za pośrednictwem interfejsu linii komend (CLI) przez port konsoli, telnet, SSH, a także za pośrednictwem interfejsu WWW.
9.	Przełącznik musi posiadać architekturę non-blocking.
10.	Przełącznik musi obsługiwać ramki Jumbo (9KB).
11.	Przełącznik musi obsługiwać sieci VLAN zgodne z IEEE 802.1q w liczbie nie mniejszej niż 4000

12.	Przełącznik musi obsługiwać sieci VLAN oparte o porty fizyczne (port-based) i adresy MAC (MAC-based). W celu automatycznej konfiguracji sieci VLAN.
13.	Przełącznik musi obsługiwać agregowanie połączeń zgodne z IEEE 802.3ad - nie mniej niż 128 grupy LAG, po nie mniej niż 16 portów.
14.	Przełącznik musi obsługiwać protokół Spanning Tree i Rapid Spanning Tree, zgodnie z IEEE 802.1D-2004, a także Multiple Spanning Tree zgodnie z IEEE 802.1Q-2003.
15.	Przełącznik musi obsługiwać protokół LLDP.
16.	Przełącznik musi obsługiwać routing między sieciami VLAN – routing statyczny, protokoły routingu dynamicznego: RIP, OSPF, IS-IS, BGP, MPLS oraz VXLAN, OVSDB. Jeżeli do realizacji tych wymagań jest wymagana licencja musi ona być dostarczona z urządzeniem
17.	Przełącznik musi obsługiwać mechanizm wykrywania awarii BFD, oraz pozwalać na stworzenie klastra HA z protokołem VRRP.
18.	Przełącznik musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3 dla ruchu wchodzącego i wychodzącego. Klasyfikacja ruchu musi odbywać się w zależności, od co najmniej: interfejsu, typu ramki Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1p), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP. Urządzenie musi obsługiwać sprzętowo nie mniej niż 8 kolejek per port fizyczny.
19.	Przełącznik musi obsługiwać filtrowanie ruchu, na co najmniej na poziomie portu i sieci VLAN dla kryteriów z warstw 2-4. Urządzenie musi realizować sprzętowo reguły filtrowania ruchu. W regułach filtrowania ruchu musi być dostępny mechanizm zliczania dla zaakceptowanych lub zablokowanych pakietów.
20.	Przełącznik musi obsługiwać takie mechanizmu bezpieczeństwa jak limitowanie adresów MAC, Dynamic ARP Inspection.
21.	Urządzenie musi obsługiwać protokół SNMP (wersje 2c i 3), oraz grupy RMON 1, 2, 3, 9. Musi być dostępna funkcja kopiowania (mirroring) ruchu na poziomie portu i sieci VLAN.
22.	Architektura systemu operacyjnego urządzenia musi posiadać budowę modularną (poszczególne moduły muszą działać w odseparowanych obszarach pamięci), m.in. moduł przekazywania pakietów, odpowiedzialny za przełączanie pakietów musi być oddzielony od modułu routingu IP, odpowiedzialnego za ustalanie tras routingu i zarządzanie urządzeniem.
23.	Urządzenie musi posiadać mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 5 poprzednich, kompletnych konfiguracji.

9.12.2 Przełączniki Data Center LAN typu LEAF - 19 szt.

Produkt musi spełnić następujące wymagania:

ID	Wymagania dla przełączników Data Center LAN typu LEAF - 19 sztuk

1.	Wymagana architektura sieci LAN musi być oparta o architekturze typu SPINE-LEAF, z podziałem ról przełączników, tworzących tzw. IP Fabric. Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do montowania w szafie rack 19''.
2.	Producent powinien oferować wsparcie dla modułów optycznych realizujących transmisję pochodzących od innych niż producent urządzeń dostawców.
3.	Przełącznik typu LEAF musi być wyposażony: - w co najmniej 48 portów 1/10GbE z minimum 12 wkładkami SFP 1000Base-T Copper Transceiver Module for up to 100m transmission on Cat5, z minimum 14 wkładkami SFP+ 10 Gigabit Ethernet Optics. - w co najmniej 6 portów 40Gbps wraz z 6 wkładkami QSFP+. Maksymalna długość kabli światłowodowych nie przekroczy 150m, a kabli miedzianych 100m.
4.	Przedstawione rozwiązanie powinno zawierać: - 19 szt. przełącznik typu LEAF oferowane urządzenia muszą zapewnić rozbudowę do co najmniej: - 24 szt. przełącznik typu LEAF
5.	Przełącznik musi posiadać wymienny zasilacz AC. Przełącznik musi być wyposażony w dodatkowy redundantny zasilacz. Musi posiadać możliwość wymiany wszystkich modułów na gorąco (hot swap). Przełączniki musza wspierać funkcjonalność ISSU.
6.	Przełącznik musi być wyposażony w port konsoli oraz dedykowany interfejs Ethernet do zarządzania OOB (out-of-band).
7.	Przełącznik musi być wyposażony w nie mniej niż 2 GB pamięci Flash oraz 2 GB pamięci DRAM. Ilość zainstalowanej pamięci RAM powinna zapewniać prawidłową pracę urządzenia oraz oprogramowania.
8.	Zarządzanie urządzeniem musi odbywać się za pośrednictwem interfejsu linii komend (CLI) przez port konsoli, telnet, SSH, a także za pośrednictwem interfejsu WWW.
9.	Przełącznik musi posiadać architekturę non-blocking.
10.	Przełącznik musi obsługiwać ramki Jumbo (9KB).
11.	Przełącznik musi obsługiwać sieci VLAN zgodne z IEEE 802.1q w liczbie nie mniejszej niż 4000
12.	Przełącznik musi obsługiwać sieci VLAN oparte o porty fizyczne (port-based) i adresy MAC (MAC-based). W celu automatycznej konfiguracji sieci VLAN.
13.	Przełącznik musi obsługiwać agregowanie połączeń zgodne z IEEE 802.3ad - nie mniej niż 128 grupy LAG, po nie mniej niż 16 portów.
14.	Przełącznik musi obsługiwać protokół Spanning Tree i Rapid Spanning Tree, zgodnie z IEEE 802.1D-2004, a także Multiple Spanning Tree zgodnie z IEEE 802.1Q-2003.
15.	Przełącznik musi obsługiwać protokół LLDP.

16.	Przełącznik musi obsługiwać routing między sieciami VLAN – routing statyczny, protokoły routingu dynamicznego: RIP, OSPF, IS-IS, BGP, MPLS oraz VXLAN, OVSDB. Jeżeli do realizacji tych wymagań jest wymagana licencja musi ona być dostarczona z urządzeniem
17.	Przełącznik musi obsługiwać mechanizm wykrywania awarii BFD, oraz pozwalać na stworzenie klastra HA z protokołem VRRP.
18.	Przełącznik musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3 dla ruchu wchodzącego i wychodzącego. Klasyfikacja ruchu musi odbywać się w zależności, od co najmniej: interfejsu, typu ramki Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1p), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP. Urządzenie musi obsługiwać sprzętowo nie mniej niż 8 kolejek per port fizyczny.
19.	Przełącznik musi obsługiwać filtrowanie ruchu, na co najmniej na poziomie portu i sieci VLAN dla kryteriów z warstw 2-4. Urządzenie musi realizować sprzętowo reguły filtrowania ruchu. W regułach filtrowania ruchu musi być dostępny mechanizm zliczania dla zaakceptowanych lub zablokowanych pakietów.
20.	Przełącznik musi obsługiwać takie mechanizmu bezpieczeństwa jak limitowanie adresów MAC, Dynamic ARP Inspection.
21.	Urządzenie musi obsługiwać protokół SNMP (wersje 2c i 3), oraz grupy RMON 1, 2, 3, 9. Musi być dostępna funkcja kopiowania (mirroring) ruchu na poziomie portu i sieci VLAN.
22.	Architektura systemu operacyjnego urządzenia musi posiadać budowę modularną (poszczególne moduły muszą działać w odseparowanych obszarach pamięci), m.in. moduł przekazywania pakietów, odpowiedzialny za przełączanie pakietów musi być oddzielony od modułu routingu IP, odpowiedzialnego za ustalanie tras routingu i zarządzanie urządzeniem.
23.	Urządzenie musi posiadać mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 5 poprzednich, kompletnych konfiguracji.

9.12.3 Router BGP - 2 szt.

GUGiK jest podłączony do sieci Internet poprzez co najmniej dwóch niezależnych operatorów. Istnieje samodzielnie zarejestrowana w RIPE jednostka, posiadająca własną adresacje IP (Provider Independent) oraz identyfikator AS.

ID	Wymagania dla Routera BGP - 2 sztuki

1.	Router musi być dedykowanym urządzeniem sieciowym o wysokości max. 4 U przystosowanym do montowania w szafie rack, wyposażonym w wymienny zasilacz oraz wentylatory. Router musi być wyposażony w zasilacze dostosowane do napięcia 220-230V, w ilości umożliwiającej poprawną pracę rutera w pełnej konfiguracji przy obsadzeniu wszystkich dostępnych slotów modułami z interfejsami.
2.	Router musi posiadać możliwość wyposażenia w nadmiarowe zasilacze w celu uzyskania redundancji zasilania 1:1.
3.	Zarządzanie i konfiguracja rutera przez administratorów musi być realizowana przez moduł kontrolny. System operacyjny rutera musi być instalowany i uruchamiany na module kontrolnym. Moduł kontrolny musi odpowiadać ze sterowanie i monitorowanie pracy komponentów urządzenia. Ruch tranzytowy użytkowników przechodzący przez ruter nie może być przesyłany przez moduł kontrolny. Moduł kontrolny musi być wyposażony w co najmniej 2 GB pamięci RAM, pamięć Flash, port konsoli oraz interfejs Ethernet służący do zarządzania out-of-band. Moduł kontrolny musi posiadać slot USB przeznaczony do podłączenia dodatkowego nośnika danych. Musi być dostępna opcja uruchomienia systemu operacyjnego rutera z nośnika danych podłączonego do slotu USB na module kontrolnym.
4.	System operacyjny routera musi posiadać budowę modułową (moduły muszą działać w odseparowanych obszarach pamięci) i zapewniać całkowitą separację płaszczyzny kontrolnej od płaszczyzny przetwarzania ruchu użytkowników, m.in. moduł routingu IP, odpowiedzialny za ustalenie tras routingu i zarządzanie urządzenia musi być oddzielony od modułu przekazywania pakietów, odpowiedzialnego za przełączanie pakietów pomiędzy segmentami sieci obsługiwanymi przez urządzenie. Obsługa ruchu tranzytowego użytkowników musi być realizowana sprzętowo.
5.	Router musi być wyposażony w 20 portów 1000Base wraz z modułami optycznymi (5*1000Base-LX, 5*1000Base-SX, 10*1000Base-TX). Router musi zapewniać pełną przepustowość dla dostarczone liczby portów dla każdej dopuszczalnej długości pakietów. Router mieć możliwość rozbudowy przepustowości do nie mniej niż 55 Mpps full duplex bez konieczności wymiany obudowy, modułów zarządzających.
6.	Router musi obsługiwać interfejsy 10 Gigabit Ethernet zgodne z IEEE 802.3ae. Router musi obsługiwać interfejsy 1 Gigabit Ethernet SFP. Urządzenia musi obsługiwać moduły SFP o prędkości 1 Gb/s. Interfejsy GbE muszą współpracować z modułami SFP pochodzącymi od innych producentów. Router musi obsługiwać ramki Jumbo o wielkości 9 KB.
7.	Porty GbE i 10 GbE urządzenia muszą obsługiwać mechanizm Digital Optical Monitoring (DOM).
8.	Urządzenie musi obsługiwać w sprzęcie routing IPv4, IPv6 oraz MPLS.
9.	Urządzenie musi obsługiwać routing statyczny IPv4 oraz routing dynamiczny IPv4 – co najmniej dla protokołów routingu OSPF, IS-IS i BGP.
10.	Urządzenie musi obsługiwać routing statyczny IPv6 oraz routing dynamiczny IPv6 – co najmniej dla protokołów routingu OSPF, IS-IS i BGP.
11.	Router jednocześnie musi obsługiwać nie mniej niż 900 tysięcy wpisów w tablicy routingu IPv4, 900 tysięcy wpisów w tablicy VPN IPv4, 700 tysięcy wpisów w tablicy routingu IPv6 oraz 128 tysięcy adresów MAC.

12.	Router musi obsługiwać mechanizm tworzenia wirtualnych ruterów (kontekstów, ruterów logicznych) umożliwiający routing pakietów w oparciu o niezależne tablice routingu – musi m.in. umożliwiać uruchomienie nie mniej niż 5 instancji routingu BGP dla różnych numerów systemów autonomicznych. Ponadto ruter musi obsługiwać sprzętowo 3 pełne tablice BGP dla IPv4 dla 3 różnych numerów systemów autonomicznych (przy założeniu, że w pełnej tablicy BGP znajduje się 300 tysięcy prefiksów). Router musi obsługiwać nie mniej niż 500 sesji BGP.
13.	Router musi obsługiwać protokół redundancji VRRP.
14.	Mechanizm BFD musi być obsługiwany dla IPv4, IPv6 oraz MPLS LSP.
15.	Urządzenie musi posiadać funkcję filtrowania ruchu wchodzącego i wychodzącego z wszystkich interfejsów. Filtrowanie ruchu musi odbywać się co najmniej na podstawie adresów MAC, IPv4 i IPv6. Router musi obsługiwać nie mniej niż 10 000 reguł filtrowania ruchu. Włączenie filtrowania nie może powodować degradacji wydajności urządzenia, tzn. musi być realizowane sprzętowo z prędkością łącza.
16.	Router musi obsługiwać protokół SNMP w wersjach 1, 2 i 3. Router musi udostępniać za pomocą protokołu SNMP co najmniej 64 bitowe liczniki ramek i bajtów wysłanych i odebranych na poszczególnych interfejsach tranzytowych. Router musi udostępniać za pomocą protokołu SNMP liczniki odebranych ramek zawierających błędy na poszczególnych interfejsach tranzytowych. Router musi udostępniać za pomocą CLI liczniki ramek wysłanych, odebranych oraz zawierających błędy na poszczególnych interfejsach tranzytowych. Ponadto po SNMP muszą być dostępne liczniki pakietów i bajtów przechwyconych przez poszczególne filtry ruchu (ACL).
17.	Router musi posiadać mechanizmy pozwalające na ograniczanie pasma dla ruchu wyjściowego i wejściowego na wszystkich interfejsach tranzytowych (z uwzględnieniem filtrów ruchu – ACL) oraz dla poszczególnych sieci VLAN.
18.	Router musi posiadać mechanizmy klasyfikowania ruchu, jego filtrowanie oraz znakowanie w oparciu co najmniej 802.1p, DSCP, ToS, MPLS EXP na wszystkich portach tranzytowych oraz dla poszczególnych sieci VLAN. Dodatkowo klasyfikacja pakietów musi się również odbywać o dane z protokołu BGP – nie mniej niż Community i AS Path. Znakowanie pakietów musi być wykonywane również przez tri-colored policer.
19.	Urządzenie musi wykonywać shaping lub policing ruchu per port.
20.	Router musi obsługiwać co najmniej 8 kolejek wyjściowych dla każdego portu tranzytowego. Urządzenie musi posiadać możliwość buforowania do 100 ms na wszystkich portach tranzytowych. Router musi obsługiwać mechanizm WRED. Router musi wspierać mechanizmy HQoS
21.	Router musi mieć zaimplementowane tunelowanie GRE oraz IP-IP bezpośrednio na karcie liniowej o wydajności przynajmniej 1Gbps.
22.	Router musi obsługiwać ruch IP multicast – w zakresie co najmniej protokołów IGMP (wersje 1, 2, 3) oraz PIM-SM.
23.	Na wszystkich interfejsach przeznaczonych do obsługi ruchu tranzytowego urządzenia musi obsługiwać usługi MPLS – nie mniej niż L2 VPN, VPLS (oparte o LDP i BGP) oraz BGP/MPLS VPN

	(L3 VPN).
24.	Router musi obsługiwać nie mniej niż 2000 sieci VPLS.
25.	Dla L2 VPN oraz VPLS musi być obsługiwany multihoming.
26.	Router musi obsługiwać protokół sygnalizacji RSVP-TE z mechanizmem Fast Reroute (node protection oraz link protection).
27.	Router musi posiadać możliwość uruchomienia mechanizmu DiffServ Traffic Engineering w celu przekierowania ruchu należącego do różnych klas obsługi ruchu na różne ścieżki MPLS.
28.	Router musi obsługiwać ruch multicast w IPVPN według draft-rosen-vpn-mcast-08.txt (lub nowszym).
29.	W ramach IPVPN ruch multicast musi być obsługiwany wykorzystując sygnalizację BGP oraz w zakresie transportu MPLS point-to-multipoint według draft-ietf-l3vpn-2547bis-mcast-bgp-03.txt (lub nowszym), draft draft-ietf-l3vpn-2547bis-mcast-02.txt (lub nowszym)., Requirements for Multicast in Layer 3 Provider-Provisioned Virtual Private Networks (PPVPNs) RFC4834 oraz draft-ietf-l3vpn-mvpn-considerations-01.
30.	Urządzenie musi obsługiwać sieci VLAN zgodnie z IEEE 802.1q. Urządzenie musi pozwalać na skonfigurowanie i uruchomienie nie mniej niż 4094 sieci VLAN jednocześnie.
31.	Urządzenie musi obsługiwać mechanizm Q-in-Q włącznie z funkcją terminowania wewnętrznych sieci VLAN na interfejsach warstwy trzeciej.
32.	Urządzenie musi obsługiwać protokoły Spanning Tree – zgodnie z co najmniej IEEE 802.1d, 802.1w i 802.1s.
33.	Ramki BPDU pomiędzy sieciami VLAN muszą być przenoszone przez urządzenie również w trybie MPLS/VPLS.
34.	Urządzenie musi obsługiwać pracę w architekturze pierścienia z możliwością przerwania pierścienia w różnych miejscach dla różnych sieci wirtualnych (np. z wykorzystaniem Per VLAN Spanning Tree Protocol). Urządzenie musi umożliwiać szybkie przywrócenie (nie dłużej niż 1 sekunda) komunikacji w pierścieniu składającym się z co najmniej 100 urządzeń.
35.	Router musi być zarządzany poprzez tekstowy interfejs linii komend (CLI) dostępny po porcie konsoli, oraz protokół Telnet i SSH dostępny przez interfejs do zarządzania out-of-band oraz dowolny interfejs tranzytowy. Router musi posiadać funkcję współpracy z zewnętrznymi serwerami AAA RADIUS (RFC 2138, RFC 2139) oraz TACACS+ (RFC 1492).
36.	Router musi posiadać funkcję limitowania pasma dla usług, których działania jest niezbędne do prawidłowego działania urządzenia, a które mogą stać się celem ataku Denial of Service.
37.	Urządzenia musi mieć domyślnie zaimplementowane zabezpieczenia przed atakami na poziomie protokołu ARP – minimalny wymagany poziom zabezpieczeń to limitowanie ruchu ARP.

9.12.4 Przełącznik LAN typu Top of the Rack - 13 szt.

ID	Wymagania dla przełączników LAN typu Top of the Rack - 13 sztuk
1.	Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do montowania w szafie rack 19''.
2.	Producent powinien oferować wsparcie dla modułów optycznych realizujących transmisję pochodzących od innych niż producent urządzeń dostawców.
3.	Przełącznik musi być wyposażony, w co najmniej 24 porty Ethernet 10/100/1000 Mb/s oraz minimum 4 porty typu SFP/SPF+ wraz z wkładkami 1/10G SFP/SFP+. Przełącznik musi umożliwiać stworzenie stosu w postaci pętli liczącego nie mniej niż 4 urządzenia. Stos musi być widoczny z punktu widzenia zarządzania, jako jedno urządzenie. Zarządzanie wszystkimi przełącznikami w stosie musi się odbywać z dowolnego przełącznika będącego częścią stosu. Stos musi być odporny na awarie, tzn. przełącznik kontrolujący pracę stosu (master) musi być automatycznie zastąpiony przełącznikiem pełniącym rolę backup – wybór przełącznika backup nie może odbywać się w momencie awarii przełącznika master. Wydajność połączenia stosu musi być nie mniejsza niż 80Gbps a pojedynczego urządzenia nie mniejsza niż 128Gbps i 95Mpps.
4.	Przełącznik musi posiadać zasilacz AC
5.	Przełącznik musi być wyposażony w port konsoli oraz dedykowany interfejs Ethernet do zarządzania OOB (out-of-band).
6.	Przełącznik musi być wyposażony w nie mniej niż 2GB pamięci Flash oraz minimum 1GB pamięci DRAM. Ilość zainstalowanej pamięci RAM powinna zapewniać prawidłową pracę urządzenia oraz oprogramowania.
7.	Zarządzanie urządzeniem musi odbywać się za pośrednictwem interfejsu linii komend (CLI) przez port konsoli, telnet, SSH, a także za pośrednictwem interfejsu WWW.
8.	Przełącznik musi obsługiwać ramki Jumbo (9KB).
9.	Przełącznik musi obsługiwać sieci VLAN zgodne z IEEE 802.1q w liczbie nie mniejszej niż 4000
10.	Przełącznik musi obsługiwać sieci VLAN oparte o porty fizyczne (port-based) i adresy MAC (MAC-based). W celu automatycznej konfiguracji sieci VLAN.
11.	Przełącznik musi obsługiwać agregowanie połączeń zgodne z IEEE 802.3ad
12.	Przełącznik musi obsługiwać protokół Spanning Tree i Rapid Spanning Tree, zgodnie z IEEE 802.1D-2004, a także Multiple Spanning Tree zgodnie z IEEE 802.1Q-2003.
13.	Przełącznik musi obsługiwać protokół LLDP.
14.	Przełącznik musi obsługiwać routing między sieciami VLAN – routing statyczny, oraz protokoły routingu dynamicznego: RIP, OSPF. Jeżeli wymagana jest licencja na wsparcie dla tych mechanizmów wymaga się jej dostarczenia minimum dla protokołu RIP v1/v2.
15.	Przełącznik musi obsługiwać mechanizm wykrywania awarii BFD (dopuszcza się jako opcję

	licencjonowaną).
16.	Przełącznik musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3 dla ruchu wchodzącego i wychodzącego. Klasyfikacja ruchu musi odbywać się w zależności, od co najmniej: interfejsu, typu ramki Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1p), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP. Urządzenie musi obsługiwać sprzętowo nie mniej niż 8 kolejek per port fizyczny.
17.	Przełącznik musi obsługiwać filtrowanie ruchu, na co najmniej na poziomie portu i sieci VLAN dla kryteriów z warstw 2-4. Urządzenie musi realizować sprzętowo reguły filtrowania ruchu. W regułach filtrowania ruchu musi być dostępny mechanizm zliczania dla zaakceptowanych lub zablokowanych pakietów.
18.	Przełącznik musi obsługiwać takie mechanizmu bezpieczeństwa jak limitowanie adresów MAC, Dynamic ARP Inspection. Pojemność tablicy forwarding musi być co najmniej rozmiaru 16000, VLAN min. 4000 a Tablica ARP min. 1024.
19.	Przełącznik musi obsługiwać IEEE 802.1x zarówno dla pojedynczego, jak i wielu suplikantów na porcie. Przełącznik musi przypisywać ustawienia dla użytkownika na podstawie atrybutów zwracanych przez serwer RADIUS, (co najmniej VLAN oraz reguła filtrowania ruchu). Musi istnieć możliwość pominięcia uwierzytelnienia 802.1x dla zdefiniowanych adresów MAC..
20.	Urządzenie musi obsługiwać protokół SNMP (wersje 2c i 3), oraz grupy RMON 1, 2, 3, 9. Musi być dostępna funkcja kopiowania (mirroring) ruchu na poziomie portu i sieci VLAN.
21.	Architektura systemu operacyjnego urządzenia musi posiadać budowę modularną (poszczególne moduły muszą działać w odseparowanych obszarach pamięci), m.in. moduł przekazywania pakietów, odpowiedzialny za przełączanie pakietów musi być oddzielony od modułu routingu IP, odpowiedzialnego za ustalanie tras routingu i zarządzanie urządzeniem.
22.	Urządzenie musi posiadać mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 5 poprzednich, kompletnych konfiguracji.

9.12.5 Przełącznik Koncentrujący Top of the Rack - 1 szt.

ID	Wymagania dla przełącznika Koncentrujący Top of the Rack - 1 sztuka
1.	Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do montowania w szafie rack 19''.
2.	Producent powinien oferować wsparcie dla modułów optycznych realizujących transmisję pochodzących od innych niż producent urządzeń dostawców.

3.	Przełącznik musi być wyposażony, w co najmniej 30 portów Ethernet typu SFP wraz z wkładkami 1 GbE SFP oraz musi umożliwiać rozbudowę o co najmniej 4 porty 10GbE lub 2 porty 40 GbE. Przełącznik musi umożliwiać stworzenie stosu nie mniej niż 8 urządzeń. Stos musi być widoczny z punktu widzenia zarządzania, jako jedno urządzenie. Zarządzanie wszystkimi przełącznikami w stosie musi się odbywać z dowolnego przełącznika będącego częścią stosu. Stos musi być odporny na awarie, tzn. przełącznik kontrolujący pracę stosu (master) musi być automatycznie zastąpiony przełącznikiem pełniącym rolę backup – wybór przełącznika backup nie może odbywać się w momencie awarii przełącznika master. Wydajność połączenia stosu musi być nie mniejsza niż 320Gbps a pojedynczego urządzenia nie mniejsza niż 450Gbps i 300Mpps.
4.	Przełącznik musi posiadać dwa zasilacz AC pracujące redundantnie
5.	Przełącznik musi być wyposażony w port konsoli oraz dedykowany interfejs Ethernet do zarządzania OOB (out-of-band).
6.	Przełącznik musi być wyposażony w nie mniej niż 2GB pamięci Flash oraz 2GB pamięci DRAM. Ilość zainstalowanej pamięci RAM powinna zapewniać prawidłową pracę urządzenia oraz oprogramowania.
7.	Zarządzanie urządzeniem musi odbywać się za pośrednictwem interfejsu linii komend (CLI) przez port konsoli, telnet, SSH, a także za pośrednictwem interfejsu WWW.
8.	Przełącznik musi obsługiwać ramki Jumbo (9KB).
9.	Przełącznik musi obsługiwać sieci VLAN zgodne z IEEE 802.1q w liczbie nie mniejszej niż 4000
10.	Przełącznik musi obsługiwać sieci VLAN oparte o porty fizyczne (port-based) i adresy MAC (MAC-based). W celu automatycznej konfiguracji sieci VLAN.
11.	Przełącznik musi obsługiwać agregowanie połączeń zgodne z IEEE 802.3ad
12.	Przełącznik musi obsługiwać protokół Spanning Tree i Rapid Spanning Tree, zgodnie z IEEE 802.1D-2004, a także Multiple Spanning Tree zgodnie z IEEE 802.1Q-2003.
13.	Przełącznik musi obsługiwać protokół LLDP.
14.	Przełącznik musi obsługiwać routing między sieciami VLAN – routing statyczny, oraz protokoły routingu dynamicznego: RIP, OSPF, BGP, IS-IS. Jeżeli wymagana jest licencja na wsparcie dla tych mechanizmów wymaga się jej dostarczenia minimum dla protokołu RIP v1/v2.
15.	Przełącznik musi obsługiwać mechanizm wykrywania awarii BFD (dopuszcza się jako opcję licencjonowaną) ,
16.	Przełącznik musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3 dla ruchu wchodzącego i wychodzącego. Klasyfikacja ruchu musi odbywać się w zależności, od co najmniej: interfejsu, typu ramki Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1p), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP. Urządzenie musi obsługiwać sprzętowo nie mniej niż 8 kolejek per port fizyczny.

17.	Przełącznik musi obsługiwać filtrowanie ruchu, na co najmniej na poziomie portu i sieci VLAN dla kryteriów z warstw 2-4. Urządzenie musi realizować sprzętowo reguły filtrowania ruchu. W regułach filtrowania ruchu musi być dostępny mechanizm zliczania dla zaakceptowanych lub zablokowanych pakietów.
18.	Przełącznik musi obsługiwać takie mechanizmu bezpieczeństwa jak limitowanie adresów MAC, Dynamic ARP Inspection. Pojemność tablicy forwarding musi być co najmniej rozmiaru 60000, VLAN min. 4000 a Tablica ARP min. 60000.
19.	Przełącznik musi obsługiwać IEEE 802.1x zarówno dla pojedynczego, jak i wielu suplikantów na porcie. Przełącznik musi przypisywać ustawienia dla użytkownika na podstawie atrybutów zwracanych przez serwer RADIUS, (co najmniej VLAN oraz reguła filtrowania ruchu). Musi istnieć możliwość pominięcia uwierzytelnienia 802.1x dla zdefiniowanych adresów MAC.
20.	Urządzenie musi obsługiwać protokół SNMP (wersje 2c i 3), oraz grupy RMON 1, 2, 3, 9. Musi być dostępna funkcja kopiowania (mirroring) ruchu na poziomie portu i sieci VLAN.
21.	Architektura systemu operacyjnego urządzenia musi posiadać budowę modularną (poszczególne moduły muszą działać w odseparowanych obszarach pamięci), m.in. moduł przekazywania pakietów, odpowiedzialny za przełączanie pakietów musi być oddzielony od modułu routingu IP, odpowiedzialnego za ustalanie tras routingu i zarządzanie urządzeniem.
22.	Urządzenie musi posiadać mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 5 poprzednich, kompletnych konfiguracji.

9.12.6 Firewall do sieci Internet - 2 szt.

ID	Wymagania podstawowe dla Firewalla do sieci Internet - 2 sztuki
1	System zabezpieczeń firewall musi być dostarczony jako dedykowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze sprzętowej systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta.
2	System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 10 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 5 Gbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering) i obsługiwać nie mniej niż 2 000 000 jednoczesnych połączeń.
3	System zabezpieczeń firewall musi być wyposażony w co najmniej 12 portów Ethernet 10/100/1000. Musi być możliwość zamontowania w urządzeniu minimum 8 interfejsów optycznych (SFP) oraz 4 interfejsów optycznych (SFP+).
4	System zabezpieczeń firewall musi działać w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer). Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA.

5	Tryb pracy urządzenia musi być ustalany w konfiguracji interfejsu sieciowego a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.).
6	System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4094 znaczników VLAN.
7	System zabezpieczeń firewall musi obsługiwać nie mniej niż 125 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF.
8	System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji.
9	Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ).
10	System zabezpieczeń firewall musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege", tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone.
11	System zabezpieczeń firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną.
12	Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż 10 Gbit/s.
13	Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM).
14	Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall.
15	Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje moduł IPS, sygnatury IPS ani dekodery protokołu IPS.
16	System zabezpieczeń firewall musi wykrywać co najmniej 1700 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS.

17	System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
18	System zabezpieczeń firewall musi posiadać możliwość definiowania i przydzielania różnych profili ochrony (AV, IPS, AS, URL, blokowanie plików) per aplikacja. Musi istnieć możliwość przydzielania innych profili ochrony (AV, IPS, AS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.
19	System zabezpieczeń firewall musi umożliwiać blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.
20	System zabezpieczeń firewall musi umożliwiać analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji.
21	System zabezpieczeń firewall musi umożliwiać ochronę przed atakami typu „Drive-by-download" poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj" dla funkcji blokowania transmisji plików.
22	System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.
23	System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej protokołem SSL dla ruchu innego niż HTTP. System musi mieć możliwość deszyfracji niezaufanego ruchu SSL i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.
24	System zabezpieczeń firewall musi umożliwiać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
	Wymagania podstawowe identyfikacja użytkowników
25	System zabezpieczeń firewall musi mieć możliwość transparentnego ustalenia tożsamości użytkowników sieci (integracja z Active Directory, Ms Exchange, Citrix, LDAP i serwerami Terminal Services). Polityka kontroli dostępu (firewall) powinna precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.

26	System zabezpieczeń firewall musi mieć możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia.
27	System zabezpieczeń firewall musi odczytywać oryginalne adresy IP stacji końcowych z nagłówka X-Forwarded-For i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesje w przypadku gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia.
	Wymagania ochrony IPS, AV, anty-spyware
28	System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
29	System zabezpieczeń firewall musi umożliwiać uruchomienie modułu inspekcji antywirusowej per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
30	System zabezpieczeń firewall musi posiadać możliwość uruchomienia modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
31	System zabezpieczeń firewall musi umożliwiać uruchomienie modułu IPS/IDS per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcjonalność IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). Wymagane dostarczenie subskrypcji na zgodny z ofertą Wykonawcy - „Czas Trwania Wsparcia Technicznego” dla funkcjonalności Intrusion Prevention System (IPS) od daty podpisania protokołu końcowego.
32	System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
33	System zabezpieczeń firewall musi posiadać moduł anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
34	System zabezpieczeń firewall musi umożliwiać uruchomienie modułu anty-spyware per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcjonalność anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
35	System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
36	System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe.

37	System zabezpieczeń firewall musi posiadać funkcjonalność podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).
38	System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.
	Wymagania dodatkowe NAT, DoS, IPSEC VPN, SSL VPN, QoS
39	System zabezpieczeń firewall musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
40	System zabezpieczeń firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
41	System zabezpieczeń firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji.
42	System zabezpieczeń firewall musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego.
43	System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.
44	System musi mieć możliwość kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. Musi istnieć możliwość przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.
	Wymagania dodatkowe środowisko wirtualne VMware
45	System zabezpieczeń firewall musi umożliwiać integrację w środowisku wirtualnym VMware w taki sposób, aby firewall mógł automatycznie pobierać informacje o uruchomionych maszynach wirtualnych (np. ich nazwy) i korzystał z tych informacji do budowy polityk bezpieczeństwa. Tak zbudowane polityki mają skutecznie klasyfikować i kontrolować ruch bez względu na rzeczywiste adresy IP maszyn wirtualnych i jakakolwiek zmiana tych adresów nie powinna pociągać za sobą konieczności zmiany konfiguracji polityk bezpieczeństwa firewalla.
	Wymagania zarządzanie i raportowanie

46	Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem.
47	System zabezpieczeń firewall musi posiadać koncept konfiguracji kandydackiej którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu.
48	System zabezpieczeń firewall musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.
49	System zabezpieczeń firewall musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).
50	Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.
51	System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos.
52	System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).
53	System zabezpieczeń firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 120 GB. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji.
54	Nie jest dopuszczalne rozwiązanie, gdzie włączenie logowania na dysk może obniżyć wydajność urządzenia.
55	System zabezpieczeń firewall musi umożliwiać usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu.
56	System zabezpieczeń firewall musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa.
57	System zabezpieczeń firewall musi posiadać możliwość konfigurowania różnych serwerów Syslog per polityka bezpieczeństwa.
58	System zabezpieczeń firewall musi mieć możliwość korelowania zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane mają zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i filtrowaniu stron www.
59	System zabezpieczeń firewall musi mieć możliwość tworzenia wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.

60	System zabezpieczeń firewall musi mieć możliwość stworzenia raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.
61	System zabezpieczeń firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.
62	Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim w autoryzowanym ośrodku edukacyjnym.

9.12.7 Urządzenia do nagrywania sesji zdalnego dostępu (appliance) - 1 szt.

ID	Urządzenia do nagrywania sesji zdalnego dostępu (appliance) wraz z konfiguracją i instalacją urządzenia - 1 sztuka
1	Rozwiązanie typu „appliance”: sprzęt + oprogramowanie
2	Rozwiązanie typu „solution in a box” - nie wymaga integracji z żadnym z istniejących elementów infrastruktury sieciowej
3	Rozwiązanie nie wymaga instalowania dodatkowego oprogramowania (agentów) na monitorowanych serwerach
4	Wspierane protokoły: - protokoły tekstowe: SSH, Telnet, Telnet 3270, - protokoły graficzne: RDP, VNC, X11, - protokoły bazodanowe: Oracle, - pozostałe protokoły: HTTP, HTTPS, Modbus.
5	Rozwiązanie pozwala na kontrolę funkcjonalności w protokołach RDP, SSH, VNC
6	Rozwiązanie posiada możliwość uwierzytelniania poprzez zewnętrzne serwery: Active Directory, LDAP, RADIUS
7	W rozwiązaniu analiza i rejestracja sesji dla ww. Protokołów odbywa się na urządzeniu, nie stosowane są „stacje przesiadkowe”
8	Rozwiązanie umożliwia synchronizację użytkowników z Active Directory, LDAP
9	W rozwiązaniu administrowanie, monitorowanie oraz podgląd sesji odbywa się poprzez przeglądarkę www
10	Rozwiązanie nagrywa cały ruch sieciowy związany z daną sesją
11	Rozwiązanie pozwala na selektywne wskazanie dla których połączeń lub grup połączeń ma być włączone nagrywanie sesji

12	Rozwiązanie umożliwia podmianę loginu i hasła wprowadzonego przez użytkownika na inny, znany na systemie docelowym
13	W rozwiązaniu podgląd monitorowanych sesji (zarówno “na żywo” jak i wcześniej nagranych) nie wymaga instalowania dodatkowego oprogramowania
14	W rozwiązaniu obraz podglądu sesji jest dynamicznie budowany w dowolnej przeglądarce z zachowanych danych sesji (nie jest to odtwarzanie statycznego zapisu wideo)
15	W rozwiązaniu, dla zapisanych sesji terminalowych (np. Telnet, ssh) istnieje możliwość interakcji z tekstem (np. Copy & paste)
16	Rozwiązanie umożliwia przerwanie monitorowanej sesji
17	Rozwiązanie umożliwia chwilowe wstrzymanie i wznowienie sesji
18	Rozwiązanie umożliwia pro-aktywny monitoring, powodujący przerwanie sesji oraz alert administratora po wykryciu zadanych komend lub ciągu znaków
19	Rozwiązanie umożliwia dołączenie się administratora do sesji telnet, SSH, RDP, VNC z poziomu przeglądarki (np. Dla wprowadzenia hasła, wpisanie polecenia systemowego)
20	Rozwiązanie umożliwia udzielenie czasowego, „ad hoc”, dostępu do pojedynczej sesji za pośrednictwem www poprzez przesłanie adresu url
21	Rozwiązanie ma możliwość konfiguracji klastrowej w trybie multi-master
22	Rozwiązanie posiada bezpieczny mechanizm inicjacji systemu oraz generowania kluczy, które nie są znane producentowi
23	Rozwiązanie umożliwia znakowanie czasem zapisanych sesji, przez kwalifikowane podmioty (Trusted Timestamping)
24	Rozwiązanie zapewnia ochronę kryptograficzną wszystkich zapisanych danych (szyfrowanie oraz integralność zapewniona poprzez sumy kontrolne)
25	Rozwiązanie posiada min 24 TB przestrzeni na dane
26	Rozwiązanie posiada 2 interfejsy sieciowe, z możliwością rozszerzenia
27	Rozwiązanie obsługuje vlany
28	Rozwiązanie posiada dokumentację oraz interfejs użytkownika w języku polskim
29	Rozwiązanie posiada wsparcie techniczne w języku polskim
30	Zapewnia możliwość uwierzytelnienia użytkownika przed urządzeniem monitorującym
31	Rozwiązanie pozwala na podłączenie się administratora do nawiązanej sesji i interakcję w ramach tej sesji
32	Obsługa klawiatury polskiej, niemieckiej, rosyjskiej i angielskiej

33	Kontrola rozdzielczości i głębi kolorów w sesjach RDP
34	Rozwiązanie współpracuje z zewnętrznymi repozytoriami haseł: Lieberman ERPM, Thycotic Secret Server, Hitachi-ID, TPAM Dell oraz cyberark
35	Rozwiązanie umożliwia podanie powodu logowania na ekranie uwierzytelniającym
36	(Bastion) - dla protokołów RDP, VNC, SSH, TELNET, TELNET_3270, rozwiązanie pozwala na uzyskanie dostępu do grupy monitorowanych serwerów poprzez jeden adres sieciowy (jedną parę IP i port) Nazwa docelowego serwera jest wskazywana w nazwie użytkownika przy użyciu separatora, np 'ssh -l user#mailserv nazwa-serwera’
37	Rozwiązanie umożliwia tagowanie i komentowanie przeglądanych sesji
38	Rozwiązanie umożliwia kontekstowe przeszukiwanie sesji
39	(Business Intelligence) rozwiązanie ma możliwość monitorowania, raportowania oraz analizy aktywności użytkownika podczas sesji (np dla oceny produktywności i/lub kontroli stopnia zaangażowania i rozliczeń z firmą zewnętrzną)
40	Rozwiązanie pozwala na współpracę z rozwiązaniem Microsoft RD Connection Broker
41	Rozwiązanie posiada wsparcie dla klawiatury polskiej, niemieckiej, rosyjskiej i angielskiej w GUI i przy podłączaniu się do sesji z poziomu przeglądarki
42	(OCR) rozwiązanie umożliwia wyszukiwania tekstu w sesjach graficznych (np RDP) dla protokołu RDP, rozwiązanie współpracuje ze stacjami wyposażonymi w kilka monitorów
43	Szczegółowe raportowanie cykliczne na podstawie własnych definicji filtrowania, upraszcza pracę osób odpowiedzialnych za nadzór infrastruktury serwerów podlegających monitorowaniu
44	Uproszczone zarządzanie czasowym dostępem do monitorowanych systemów dzięki możliwości zdefiniowania ram czasowych ważnych kont użytkowników
45	Możliwość eksportowania I importowania konfiguracji (ustawienia sieciowe, adresy IP, definicje użytkowników, serwerów I połączeń) pozwalające na szybkie zainicjowanie maszyny zastępczej
46	Usprawnienia w zarządzaniu dużą liczbą użytkowników, upraszczające pracę osoby odpowiedzialnej za konfiguracje system
47	Szybsza analiza zarejestrowanego materiału dzięki możliwości przeskakiwania pomiędzy wystąpieniami wyszukiwanej frazy
48	Filtrowanie wpisów dziennika zdarzeń według obiektów, których dotyczą pozwala na sprawniejszy audyt
49	Płynne współdzielenie sesji, wspólna praca na 2 pary oczu
50	Dostępne 4 tryby pracy: bastion, proxy, gateway, bridge
51	Ochrona przed wyłączeniem serwera zdalnego

52	Harmonogram generowania raportów i wysyłania mailem
53	Licencja na minimum 1500 hostów

9.12.8 Firewall Data Center - 2 szt.

Nr.	Wymagania podstawowe dla Firewalla Data Center - 2 sztuki
1.	Firewall musi być dostarczony w postaci dwóch dedykowanych urządzeń typu appliance, przystosowanych do montażu w szafie rack, wyposażonych w pasywny midplane, wymienne wentylatory oraz 1 źródło zasilania AC. Ponadto urządzania muszą być wyposażone w nadmiarowe źródło zasilania w celu zapewnienia redundancji zasilania 1:1.
2.	Firewall musi posiadać wymienne karty z matrycą przełączającą, karty z interfejsami sieciowymi oraz karty usługowe realizujące sprzętowo funkcje bezpieczeństwa.
3.	Firewall musi posiadać 1 slot przeznaczony wyłącznie na kartę z matrycą przełączającą Karta z matrycą przełączającą musi posiadać wewnętrzne połączenie z wszystkimi kartami z interfejsami sieciowymi oraz wszystkimi kartami usługowymi.
4.	Zarządzanie i konfiguracja firewalla przez administratorów musi być realizowana przez moduł kontrolny. System operacyjny firewalla musi być instalowany i uruchamiany na module kontrolnym. Moduł kontrolny musi odpowiadać za sterowanie i monitorowanie pracy komponentów firewalla. Ruch tranzytowy użytkowników przechodzący przez firewall nie może być przesyłany przez moduł kontrolny. Moduł kontrolny musi posiadać slot USB przeznaczony do podłączenia dodatkowego nośnika danych. Musi być dostępna opcja uruchomienia systemu operacyjnego firewalla z nośnika danych podłączonego do slotu USB na module kontrolnym.
5.	System operacyjny firewalla musi posiadać budowę modułową (moduły muszą działać w odseparowanych obszarach pamięci) i zapewniać całkowitą separację płaszczyzny kontrolnej od płaszczyzny przetwarzania ruchu użytkowników, m.in. moduł rutingu IP, odpowiedzialny za ustalenie tras rutingu i zarządzanie urządzenia musi być oddzielony od modułu przekazywania pakietów, odpowiedzialnego za przełączanie pakietów pomiędzy segmentami sieci obsługiwanymi przez urządzenie. Obsługa ruchu tranzytowego użytkowników musi być realizowana sprzętowo. System operacyjny firewalla musi śledzić stan sesji użytkowników (stateful processing), tworzyć i zarządzać tablicą stanu sesji. System operacyjny Firewall musi umożliwiać dostęp z zewnętrznych aplikacji poprzez mechanizmy API XML
6.	Firewall musi obsługiwać co najmniej następujące rodzaje kart z interfejsami sieciowymi: Nie mniej niż 10 portów 10GE SFP+ Możliwość rozbudowy o 10 portów 10GE Możliwość rozbudowy o port 100GE Możliwość rozbudowy o port 20 portów 1GE
7.	Firewall musi umożliwiać zainstalowanie nie mniej niż 3 kart z interfejsami sieciowymi (z możliwością rozbudowy do co najmniej 4 kart).

	Karty muszą posiadać przepustowość co najmniej 10 Gb/s full duplex. Każde z urządzeń musi być dostarczone z kartą wyposażoną w dwa interfejsy 10 GbE .
8.	Mechanizmy QoS (policing, kolejkowaniem, shaping) oraz funkcje ochrony przed atakami DoS i DDoS muszą być realizowane sprzętowo.
9.	Realizacja mechanizmów bezpieczeństwa musi się odbywać na wyspecjalizowanych kartach usługowych posiadających własny procesor. Karty usługowe muszą realizować sprzętowo co najmniej takie funkcje jak stateful firewall, translacja adresów IP, IPSec VPN, oraz po opcjonalnej rozbudowie: intrusion prevention (IPS), oraz cechy next generation firewall w zakresie identyfikacji i sterowania aplikacji sieciowych jak m.in. Skype, BitTorrent. Wszystkie karty usługowe muszą posiadać identyczną funkcjonalność i pracować pod kontrolą systemu operacyjnego firewalla – nie dopuszcza się możliwości realizacji całości lub części ww. funkcji bezpieczeństwa przez karty działające pod kontrolą innych systemów operacyjnych. Zwiększenie wydajności ww. funkcji bezpieczeństwa musi się odbywać przez zwiększanie ilości kart usługowych. Firewall musi posiadać minimum 6 slotów pozwalających na zainstalowanie i uruchomienie kart usługowych. Nie dopuszcza się również sytuacji, aby poszczególne moduły usługowe były traktowane przez system operacyjny firewalla jako niezależne urządzenia, z osobnymi regułami polityki firewall – z punktu widzenia systemu operacyjnego firewalla wszystkie moduły usługowe muszą być integralną częścią urządzenia i wszystkie muszą podlegać tej samej polityce bezpieczeństwa konfigurowanej na module kontrolnym.
10.	Firewall (dla każdego urządzenia) : • musi realizować zadania Stateful Firewall z mechanizmami ochrony przed atakami DoS, wykonując kontrolę na poziomie sieci oraz aplikacji pomiędzy nie mniej niż 256 strefami bezpieczeństwa z sumaryczną wydajnością nie mniejszą niż 200 Gb/s liczoną dla dużych pakietów. • musi obsłużyć sumarycznie nie mniej niż 1mln równoległych sesji lub zestawić sumarycznie nie mniej niż 100 tysięcy nowych połączeń/sekundę. • jednocześnie musi istnieć możliwość rozbudowy by obsługiwało dla funkcji Stateful Firewall co najmniej przepustowość 400 Gb/s dla dużych pakietów i 2mln sesji równoległych.
11.	Firewall musi zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site. IPSec VPN musi być realizowany sprzętowo przez karty usługowe. Firewall musi obsłużyć nie mniej niż 14 000 równoległych tuneli VPN oraz ruch szyfrowany o przepustowości nie mniej niż 3 Gb/s dla pakietów typu IMIX.
12.	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, użytkowników aplikacji, reakcje zabezpieczeń oraz metody rejestrowania zdarzeń. Firewall musi umożliwiać zdefiniowanie nie mniej niż 35 000 reguł polityki bezpieczeństwa.

13.	Firewall ma umożliwiać rozbudowę o funkcje wykrywania i blokowania ataków intruzów (IPS, intrusion prevention) oraz ochrony aplikacji (Application Security) realizowanej sprzętowo lub programowo na modułach usługowych. System zabezpieczeń musi wtedy identyfikować próby skanowania, penetracji i włamań, ataki typu exploit (poziomu sieci i aplikacji), ataki destrukcyjne i destabilizujące (D)DoS oraz inne techniki stosowane przez hakerów. Ustalenie blokowanych ataków (intruzów, robaków) musi odbywać się w regułach polityki bezpieczeństwa. System firewall musi realizować zadania IPS z sumaryczną wydajnością nie mniejszą niż 8 Gb/s. Baza sygnatur IPS musi być utrzymywana i udostępniana przez producenta urządzenia firewall, zawierać co najmniej 6000 sygnatur ataków. Baza sygnatur ataków musi być aktualizowana przez producenta co najmniej raz w tygodniu. Wymagane dostarczenie subskrypcji na zgodny z ofertą Wykonawcy - „Czas Trwania Wsparcia Technicznego" dla funkcjonalności Intrusion Prevention System (IPS) oraz ochrony aplikacyjnej od daty podpisania protokołu końcowego.
14.	Urządzenia muszą obsługiwać protokoły dynamicznego routingu: RIP, OSPF oraz BGP. Urządzenie musi obsługiwać nie mniej niż 2 000 peer'ów BGP i nie mniej niż 1 000 000 prefiksów BGP (w RIB). Urządzenia muszą umożliwiać skonfigurowanie nie mniej niż 256 wirtualnych ruterów oraz 4000 sieci VLAN z tagowaniem 802.1Q i min. 20 wirtualnych systemów.
15.	Firewall musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym QoS – wygładzanie (shaping) oraz obcinanie (policing) ruchu. Mapowanie ruchu do kolejek wyjściowych musi odbywać się na podstawie DSCP, IP ToS, 802.1p, oraz parametrów z nagłówków TCP i UDP. Urządzenia muszą posiadać tworzenia osobnych kolejek dla różnych klas ruchu. Urządzenia muszą posiadać zaimplementowany mechanizm WRED w celu przeciwdziałania występowaniu przeciążeń w kolejkach.
16.	Firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie dla urządzeń zabezpieczeń. Urządzenia zabezpieczeń w klastrze muszą funkcjonować w trybie Active-Passive, Active/Active z synchronizacją konfiguracji i tablicy stanu sesji. Przełączenie pomiędzy urządzeniami w klastrze HA musi się odbywać przezroczyście dla sesji ruchu użytkowników. Mechanizm ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. Klaster HA musi posiadać redundantne połączenia służące do synchronizacji konfiguracji i tablicy stanu sesji firewalli.
17.	Zarządzanie urządzeniem musi odbywać się za pomocą graficznej konsoli Web GUI oraz z wiersza linii poleceń (CLI) poprzez port szeregowy oraz protokoły telnet i SSH. Firewall musi posiadać możliwość zarządzania i monitorowania przez centralny system zarządzania i monitorowania pochodzący od tego samego producenta. Zarządzanie CLI obu węzłów klastra musi się odbywać z pojedynczego miejsca – konsoli jednego z węzłów (jeden plik konfiguracyjne na oba węzły klastra Firewall).
18.	Administratorzy muszą mieć do dyspozycji mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 5 poprzednich, kompletnych konfiguracji, w tym musi istnieć możliwość wskazania jednej z wersji konfiguracji jako bazowej, służącej odtworzeniu przy pomocy pojedynczej komendy konfiguracji tzw. minimalnej (nie fabrycznej).
19.	Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone są w języku polskim.

9.13 Narzędzia wspierające

9.13.1 Narzędzie do monitorowania infrastruktury SIG oraz aplikacji dedykowanych

Wszystkie licencje mają być dostarczone wraz z wsparciem technicznym, z czasem trwania wsparcia technicznego, zgodnym z ofertą Wykonawcy - „Czas Trwania Wsparcia Technicznego", świadczonym przez producenta będącego licencjodawcą oprogramowania, które powinno umożliwiać zgłaszanie problemów oraz pobieranie i instalowanie nowych poprawek, wersji oprogramowania.

ID	Narzędzie do monitorowania
1.	Oprogramowanie systemu monitorowania musi pracować w oparciu o system operacyjny Linux lub MS Windows.
2.	Oprogramowanie systemu monitorowania musi umożliwiać monitorowanie co najmniej: 1500 elementów (urządzeń sieciowych, serwerów fizycznych, serwerów wirtualnych, aplikacji, baz danych (za jeden element uznaje się rozwiązanie posiadające adres IP) W interfejsie GUI oprogramowanie systemu monitorowania musi wspierać przeglądarki WWW: Internet Explorer i Firefox. Konfiguracja oprogramowania systemu monitorowania musi się odbywać poprzez stronę www oraz programistyczne, udokumentowane API. Oprogramowanie musi umożliwiać monitorowanie podstawowych parametrów sprzętowych bez użycia dodatkowych agentów oraz pozostałe parametry działania systemu operacyjnego i usług za pomocą dedykowanych agentów (w zależności od konfiguracji monitorowanego hosta).
3.	Oferowane oprogramowanie systemu monitorowania musi śledzić parametry: - Telnet na wybrany port - nasłuch na porcie - Ping dostępność urządzenia - Poprawne działanie serwera DHCP - Poprawne działanie serwera czasu NTP - Zajętość danych na poszczególnych partycjach - Zajętość RAM - Obciążenie systemu - Obciążenie dysków

	- Ilość zalogowanych użytkowników - Ilość procesów - Obecność procesów w systemie - Synchronizacja dysków programowego RAID - Synchronizacja dysków sprzętowego RAID - Kontrola parametrów polecenia VMSTAT - Obecność SSH
4.	Oferowane oprogramowanie systemu monitorowania musi śledzić parametry monitoringu systemu poczty: • Poprawne działanie serwera SMTP • Poprawne działanie serwera POP3 • Poprawne działanie serwera IMAP • Poprawne działanie serwera AMAVIS • Ilość listów w kolejkach serwera Postfix
5.	Oferowane oprogramowanie systemu monitorowania musi śledzić parametry monitoringu DNS: • Poprawne działanie DNS • Rozwiązywanie zadanych domen na adresy IP • Parametry serwerów WWW • Poprawne działanie serwera WWW • Kontrola występowania oczekiwanych treści na stronie • Czas odpowiedzi serwera WWW.
6.	Oferowane oprogramowanie systemu monitorowania musi śledzić parametry monitoringu bazy danych: • Poprawna praca bazy • Kontrola stanu synchronizacji baz • Zajętość przestrzeni danych
7.	Oferowane oprogramowanie systemu monitorowania musi śledzić parametry DRBD i HEARTBEAT : • Poprawne działanie klastra
	• Poprawne działanie replikacji danych

8.	Oferowane oprogramowanie systemu monitorowania musi śledzić parametry macierzy dyskowych: • Analiza statusów ogólnych urządzenia, • Analiza dysków urządzenia
9.	Oferowane oprogramowanie systemu monitorowania musi posiadać możliwość personalizacji podstawowego ekranu aplikacji w powiązaniu z użytkownikiem systemu, a także umożliwiać dowolną konfigurację składników wyświetlanych na podstawowym ekranie aplikacji poprzez wybór odpowiednich widget'ów.
10.	Tworzenie i modyfikacja raportów musi być wykonywana za pośrednictwem interfejsu WWW i nie może wymagać instalacji dodatkowego oprogramowania (poza przeglądarką i ew. technologiami Java, Flash i podobnymi). Funkcjonalność tworzenia i modyfikacji raportów nie może wymagać zakupu dodatkowych licencji.
11.	Narzędzie raportujące musi umożliwiać automatyczną generację dowolnych raportów wg zdefiniowanego harmonogramu: • Możliwość generowania raportów dostępności (wg hostów lub usług) • Możliwość generowania raportów SLA (wg hostów lub usług) • Zapis raportów do plików PDF • Okresowe wysyłanie raportów emailem do wskazanych użytkowników • Zapis zdefiniowanych parametrów raportów celem późniejszego wywołania
12.	Oprogramowanie systemu monitorowania musi mieć możliwość grupowania monitorowanych elementów: • Możliwość grupowania hostów / usług w procesy biznesowe i monitorowania dostępności procesu jak pojedynczego elementu • Wykonywanie operacji na grupach hostów / usług (komentarze, powiadomienia, potwierdzenia błędów, przerwy serwisowe).
13.	Oferowane oprogramowanie systemu monitorowania musi posiadać funkcje związane z bezpieczeństwem systemu: • Wbudowany mechanizm tworzenia kopii zapasowych ustawień systemu (monitorowane hosty i usługi), • Wbudowany mechanizm zarządzania użytkownikami systemu,
	• Możliwość tworzenia grup użytkowników, • Mechanizm przydzielania uprawnień użytkowników (dostęp do danych nt. hostów lub usług, możliwość konfiguracji obiektów, powiadomienia).
14.	Oferowane oprogramowanie systemu monitorowania musi posiadać możliwość globalnego wyłączania powiadomień w systemie.

15.	Oferowane oprogramowanie systemu monitorowania musi posiadać możliwość rozbudowy o kolejne węzły.
16.	Oferowane oprogramowanie systemu monitorowania musi posiadać możliwość rozbudowy o elementy niezawodnościowe oraz elementy sond. Tak wykonana instalacja musi podlegać centralnemu zarządzaniu z poziomu interfejsu www i z poziomu jednego systemu.
17.	Oferowane oprogramowanie systemu monitorowania musi istnieć jako gotowy produkt komercyjny oraz być dostępne w oficjalnej dystrybucji na terenie Polski.
18.	Oferowane oprogramowanie systemu monitorowania musi posiadać oficjalne, nielimitowane wsparcie producenta. Nie jest akceptowalne wsparcie typu „community support", oferowane przez społeczność jego użytkowników.
19.	Oferowane oprogramowanie systemu monitorowania musi posiadać oficjalne wsparcie na mocy współpracy z dostawcą oprogramowania, którego co najmniej pierwsza linia jest świadczona w języku polskim.
20.	Oprogramowanie musi być opatrzone licencją i ścieżką rozwoju producenta.
21.	Oprogramowanie musi umożliwiać konfigurację w zakresie pozyskiwania parametrów dotyczących aplikacji dedykowanych: 1. Aktywność aplikacji Rozumiana jako bieżąca informacja która aplikacja działa a która nie. 2. Dostępność aplikacji Rozumiana jako stosunek ilości czasu w którym wybrana aplikacja jest dostępna w wybranym okresie do ilości czasu (total) w wybranym okresie. Zbieranie i przechowywanie statystyk powinno pozwalać na prezentowanie dostępności w ujęciu godzinowym, dziennym, tygodniowym, miesięcznym, rocznym 3. Wydajność aplikacji Rozumiana jako czas odpowiedzi wybranej aplikacji, wyrażony w sekundach 4. Przepustowość aplikacji Rozumiana jako ilość połączeń z aplikacją w jednostce czasu - na sekundę 5. Lista użytkowników aplikacji bieżąca i historyczna w wybranym okresie czasu (miesięcznym, rocznym) 6. Rozkład użytkowników aplikacji w kontekście dostępności do wybranych funkcjonalności aplikacji. Statystyka bieżąca i historyczna w wybranym okresie czasu (miesięcznym, rocznym) 7. Rozkład użytkowników aplikacji w kontekście przynależności do jednostek administracyjnych 8. Aktywność użytkowników aplikacji Rozumiana jako zestawienie użytkowników, aktywnie korzystających (logujących) z usługi w danym okresie. Zbieranie i przechowywanie statystyk powinno pozwalać na prezentowanie wartości parametru w ujęciu dziennym, tygodniowym, miesięcznym, rocznym. 9. Godzinowe obciążenie aplikacji Rozumiane jako ilość połączeń z aplikacją w jednostce czasu – godzina. 10. Podstawowe funkcjonalności i ich realizacja przez aplikacje Rozumiane jako zestawienie aplikacji i realizowanych przez nie funkcjonalności w kontekście biznesowym 11. Zasoby sprzętowo – systemowe niezbędne do działania aplikacji

	Rozumiane jako zestawienie niezbędnych zasobów sprzętowo-systemowych do działania aplikacji. 12. Niestandardowe zachowania aplikacji Rozumiany jako rejestr zdarzeń niestandardowego zachowania się aplikacji. Zbieranie i przechowywanie statystyk powinno pozwalać na prezentowanie wartości parametru w ujęciu dziennym, tygodniowym, miesięcznym, rocznym. 13. Incydenty i problemy zgłaszane do aplikacji Realizacja po stronie narzędzi ITSM

9.13.2 System analizy ruchu sieciowego i wykrywania anomalii

Wszystkie licencje mają być dostarczone wraz z wsparciem technicznym, z czasem trwania wsparcia technicznego, zgodnym z ofertą Wykonawcy - „Czas Trwania Wsparcia Technicznego", świadczonym przez producenta będącego licencjodawcą oprogramowania, które powinno umożliwiać zgłaszanie problemów oraz pobieranie i instalowanie nowych poprawek, wersji oprogramowania.

ID	System analizy ruchu sieciowego i wykrywania anomalii
1.	System musi analizować dane statystyczne (czyli próbki ruchu, flow-y, sample) generowane przez urządzenia sieciowe różnych producentów. System musi obsługiwać co najmniej następujące formaty próbek ruchu: Netflow (wersje 5, 7, oraz 9), Sampled Netflow, IPFIX, J-Flow, sFlow, Netstream.
2.	System musi analizować kopię ruchu sieciowego udostępnianą przez sesje port mirroringu zdefiniowane na przełącznikach Ethernet, lub przy pomocy dedykowanych sprzętowych trapów sieciowych.
3.	System musi udostępniać funkcję aktywnego tworzenia próbek ruchu z analizowanej kopii ruchu sieciowego. Musi istnieć możliwość aktywnego tworzenia próbek ruchu w formatach co najmniej Netflow v5, Netflow v9, IPFIX. System musi posiadać funkcję wysyłania aktywnie tworzonych próbek ruchu do systemu NBAD tego samego producenta oraz do kolektorów innych producentów.
4.	System musi wykrywać nowe hosty pojawiające się w sieci teleinformatycznej. System musi zbierać i przechowywać informacje o MAC adresach komputerów oraz o przypisanych do nich adresów IPv4 i IPv6.
5.	System musi posiadać funkcję pobierania informacji o działających w sieci aktywnych urządzeniach przez protokół SNMP – co najmniej nazw urządzeń, listy interfejsów sieciowych z ich nazwami, opisami i prędkościami.
6.	System musi utrzymywać centralne repozytorium informacji o analizowanym ruchu sieciowym otrzymywanych z innych urządzeń sieciowych lub własnych komponentów. Dane muszą być przechowywane w bazie danych SQL. Musi istnieć możliwość wydawania zapytań bezpośrednio do bazy danych.

7.	System musi udostępniać graficzny interfejs użytkownika do przetwarzania zebranych danych, w tym wyliczania statystyk i generowania raportów. Statystyki i raporty muszą być dostępne na bieżąco w czasie rzeczywistym.
8.	System kolekcjonowania danych musi przechowywać informacje o czasie rozpoczęcia i zakończenia strumienia analizowanych danych z dokładnością do 1 milisekundy.
9.	System musi posiadać funkcje tworzenia profili i widoków analizowanych danych, aktualizowanych na bieżąco, na podstawie kryteriów zdefiniowanych przez administratora.
10.	System musi generować raporty pokazujące dane w formie graficznej (wykresy) jak i tabelarycznej, w oparciu o kryteria wprowadzane przez użytkowników w formie filtrów. Raporty muszą obejmować również informacje o wszystkich konwersacjach pomiędzy monitorowanymi hostami.
11.	System musi udostępniać statystyki obciążenia sieci przez: · adresy i sieci IP (źródłowe i docelowe), · aplikacje (protokoły, porty źródłowe, docelowe), · klasy ruchu QoS (ToS/DSCP), · systemy autonomiczne BGP (AS), · kraje rozpoznawane na podstawie sieci IP (dla adresów źródłowych i docelowych) · ruch z określonymi flagami TCP, · protokoły IPv4 oraz IPv6.
12.	System musi generować raporty zgodnie z kryteriami ustalanymi przez administratorów oraz na podstawie predefiniowanych wzorców. Raport musza być tworzone w różnych formatach – minimum PDF i CSV. Użytkownik musi posiadać wpływa na układ raportu poprzez dobór ilości i rodzaju informacji, z których raport będzie się składał.
13.	System musi posiadać funkcję automatycznego rozwiązywania adresów IP do nazw domenowych.
14.	System musi posiadać funkcję nadawania nazw własnych następującym zaobserwowanym obiektom: · podsieciom, · aplikacjom (adresom IP i portom), · systemom autonomicznym BGP (AS).

15.	System musi udostępniać zbiorcze dane statystyczne zawierające sumaryczną liczbę otrzymanych eksportów próbek ruchu określonego typu wysłanych przez każde z urządzeń, wraz z informacjami na temat średniej oraz szczytowej liczby otrzymywanych eksportów od każdego z urządzeń.
16.	System musi pozwalać na definiowania alarmów, które będą powiadamiać administratora o ruchu sieciowym (globalnym oraz z wybranych sieci, protokołów i aplikacji) przekraczającym zdefiniowane wartości progowe wyrażone w jednostkach ilości danych (pakietach oraz bajtach), a także w jednostkach prędkości transmisji (bitach/sekundę, pakietach/sekundę).
17.	Alarmy muszą być wysyłane przy wykorzystaniu co najmniej następujących metod: syslog, e-mail, SNMP trap, komunikaty SMS (w typ przypadku dopuszcza się możliwość integracji z zewnętrzną bramką SMS).
18.	System musi posiadać możliwość uruchomienia funkcji NBAD (Network Behavior Anomaly Detection).
19.	System musi posiadać możliwość analizy stanu i efektywności działania sieci teleinformatycznej, w tym również wykrywania sytuacji nieprawidłowych (tj. anomalii) związanych z kondycją sieci oraz stanem jej bezpieczeństwa.
20.	System musi posiadać możliwość wykrywania anomalii w działaniu sieci teleinformatycznej za pomocą analizy statystycznej i behawioralnej. W tym celu system musi na bieżąco budować profile normalnego stanu i zachowania sieci oraz identyfikować odchylenia od stanu normalnego – poprzez zaobserwowanie zwiększenia lub zmniejszenie natężenia ruchu sieciowego oraz przekraczanie zdefiniowanych wartości progowych.
21.	System musi posiadać możliwość wykrywania ataków Denial of Service i Distributed Denial of Service.
22.	System musi działać w architekturze standalone – kluczowe funkcje, czyli zbieranie danych, analiza zdarzeń oraz wykrywanie anomalii muszą być wykonywane na tym samym urządzeniu.
23.	W celu zwiększenia skalowalności systemu musi istnieć możliwość uruchomienia systemu w architekturze rozproszonej, poprzez uruchomienie funkcji zbierania danych, a także ich wstępnej analizy na dedykowanych kolektorach.
24.	System musi działać pod kontrolą dostrojonego przez producenta systemu operacyjnego klasy Unix. Nie jest dopuszczalne zastosowanie systemu operacyjnego klasy Microsoft Windows.
25.	System musi posiadać wydajność analizy nie mniej niż 100 flow próbek ruchu na sekundę.
26.	System musi zbierać dane z wydajnością nie mniejszą niż 75 000 próbek ruchu na sekundę (flow-ów/sekundę). System nie może posiadać ograniczeń co do liczby obsługiwanych urządzeń będących źródłami informacji.
27.	System musi być dostarczony jako rozwiązanie gotowe do użytku, pochodzące od jednego producenta. Nie jest dopuszczalna sytuacja, w której funkcje wymagane dla systemu realizowane są przez zestaw programów pochodzących od różnych producentów, działających na tej samej platformie sprzętowej ogólnego przeznaczenia.

28.	System musi być kompletny tzn. zawierać wszystkie licencje i zezwolenia, niezbędne do poprawnego funkcjonowania zgodnie z niniejszą specyfikacją, bez konieczności wnoszenia dodatkowych.
29.	Pełne zarządzanie systemem, analiza danych oraz raportowanie musi odbywać się poprzez graficzny interfejs użytkownika dostępny za pomocą standardowych przeglądarek WWW. Nie jest dopuszczalne zarządzanie przy pomocy dodatkowych aplikacji klienckich.
30.	System musi pozwalać na definiowanie kont administratorów o zróżnicowanym poziomie uprawnień w zakresie co najmniej: pełnej kontroli nad systemem, kontroli na poszczególnymi modułami funkcjonalnymi systemu, kont uprawnionych tylko do odczytu. Ponadto musi istnieć funkcja ograniczania uprawnień kont użytkowników do poszczególnych źródeł informacji (tj. urządzeń sieciowych generujących próbki ruchu) oraz do zbioru danych definiowanych na podstawie kryteriów z warstwy 3 i 4 modelu ISO. Tożsamość administratorów musi być weryfikowana w lokalnej bazie danych użytkowników, a także przy pomocy zewnętrznych serwerów uwierzytelniania – co najmniej LDAP.
31.	Musi być dostępna funkcja zapisywania i odtwarzania pełnej konfiguracji systemu oraz jedynie wybranych jego komponentów. Musi być dostępna funkcja wykonania kopii zapasowej systemu uwzględniającej konfigurację i ewentualne licencje.
32.	System musi posiadać narzędzia do: · informowania o statusie systemu, zajętości pamięci, dostępności przestrzeni dyskowej, · konfiguracji interfejsów sieciowych, · zapisywania pełnego dziennika zdarzeń (logów) związanych z działaniem systemu i uruchomionym na nim usług.

9.13.3 Narzędzie do przechowywania, wizualizacji, wyszukiwania i analizy logów

Wszystkie licencje mają być dostarczone wraz z wsparciem technicznym, z czasem trwania wsparcia technicznego, zgodnym z ofertą Wykonawcy - „Czas Trwania Wsparcia Technicznego”, świadczonym przez producenta będącego licencjodawcą oprogramowania, które powinno umożliwiać zgłaszanie problemów oraz pobieranie i instalowanie nowych poprawek, wersji oprogramowania.

ID	Parametry minimalne wymagane przez Zamawiającego Narzędzie do przechowywania, wizualizacji, wyszukiwania i analizy logów.
1	ZBIERANIE DANYCH:
	Oprogramowanie musi pozwalać na: - zbieranie logów przesyłanych przez systemy operacyjne(Linux/Windows), urządzenia sieciowe oraz aplikacje - zbieranie danych przesyłanych po sieci (UDP/TCP), oprogramowanie musi rozpoznawać dane przesyłane przez syslog, ng-syslog, netflow.

	- zbieranie danych ekstrahowanych z plików logów umieszczonych w wyszczególnionym katalogu na serwerze z oprogramowaniem - oprogramowanie musi być uzupełnione programami klienckimi przeznaczonymi na aktualne wersje systemów operacyjnych z rodziny Linux i z rodziny Windows, które można konfigurować na okoliczność zbierania danych o stanie i zdarzeniach występujących w danym systemie operacyjnym - oprogramowanie musi być przygotowane na odbiór, indeksowanie i przetwarzanie nielimitowanej liczby zdarzeń w ramach wydajności pojedynczego serwera na którym pracuje
2	PRZECHOWYWANIE i PARSOWANIE DANYCH:
	Oprogramowane musi : - posiadać wbudowany mechanizm kompresji przechowywanych danych - pozwalać na uniwersalne parsowanie przesyłanych danych - pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych - pozwalać na rozpoznanie formatów czasu i daty, i normalizowanie ich do jednego wspólnego formatu Oprogramowanie musi umożliwiać operatorowi oprogramowania samodzielne konfigurowanie parsowania nieznanych formatów logów w celu umożliwienia analizy zebranych w nich informacji przez opisywane oprogramowanie. System ma przechowywać zbierane zdarzenia przez minimum 3 miesiące (dostępne do odczytu przez narzędzie w trybie „na żywo") oraz 1 rok (archiwizacja – dane historyczne).
3	PRZESZUKIWANIE ZEBRANYCH DANYCH
	Oprogramowanie musi być obsługiwane z poziomu przeglądarki.
	Oprogramowanie musi pozwalać na wyszukiwanie w całym zgromadzonym przez nie zbiorze danych.
	Oprogramowanie musi pozwalać na równoległe wyszukiwanie, z poziomu jednego interfejsu graficznego, w danych napływających w czasie rzeczywistym i danych historycznych.
	Oprogramowanie musi pozwalać na użycie operatorów boolowskich, wzorców, wyrażeń regularnych (REGEX) do przeszukiwania danych. Oprogramowanie musi pozwalać na przeszukiwania w ograniczonym zbiorze danych (np. ze względu na zakres dat wystąpienia).
	Oprogramowanie musi wraz z wyświetleniem wyszukiwanych wyników przedstawiać na tym samym ekranie związaną z tym wyszukiwaniem statystykę ilościową w dziedzinie czasu.
	Oprogramowanie musi pozwalać na oznaczanie (tag) i korelacje danych (pod kątem dowolnej z przechowywanych wartości) bez względu na źródło tych danych.
	Oprogramowanie wraz z prezentacją (wykres, tabela) zestawień zbiorczych, statystycznych itd. musi pozwalać na obejrzenie danych źródłowych w ich oryginalnym formacie (logi) na podstawie których powstała ta prezentacja.
	Oprogramowanie musi pozwalać na geolokalizację zdarzeń na bazie adresów IP oraz umożliwiać jej wizualizacje na mapie.
	Musi istnieć możliwość wyszukiwania na podstawie jednoczesnego wykorzystania więcej niż jednego zdefiniowanego wzorca wyszukiwania.
	Musi istnieć możliwość zapisania wyników wyszukiwania i tworzenia z nich raportów.
	Oprogramowanie musi oferować także udokumentowany interfejs programistyczny (API) służący do przeszukiwania danych gromadzonych w czasie rzeczywistym oraz danych historycznych.
	Oprogramowanie musi oferować pełne sterowanie pracą dziennika zdarzeń poprzez API.
4	Eksport danych
	Oprogramowanie musi pozwalać na eksport wyszukanych danych do formaty CSV.

5	RAPORTOWANIE
	Oprogramowanie musi dawać : - możliwość tworzenia raportów z predefiniowanych wyszukiwań w postaci tabelarycznej i graficznej (minimum 3 typy wykresów (line, bar, pie). - możliwość równoległego użycia wielu predefiniowanych wyszukiwań w celu opracowania raportu.
6	GLOWNY INTERFEJS OPROGRAMOWANIA
	Oferowana przez oprogramowanie strona www musi być zabezpieczona hasłem
	Oprogramowanie musi wspierać pracę wielu użytkowników, posiadających własne loginy i hasła
	Oprogramowanie musi posiadać dedykowany widok zarządzania użytkownikami.
	Oprogramowanie musi udostępniać funkcjonalność podziału uprawnień pomiędzy użytkownikami, co pozwoli na ograniczenie dostępu użytkowników do poszczególnych zgromadzonych danych. W systemie musi być wprowadzony mechanizm bezpieczeństwa który kontroluje jaki użytkownik ma dostęp do jakiego fragmentu danych. Mechanizm konfiguracji uprawnień musi być dostępny w poziomu www aplikacji jak i z API.
7	INTEGRACJA Z IT TOOLS
	Oprogramowanie musi udostępniać API pozwalające na integracje z innymi narzędziami służącymi do zarządzania i analizy danych
8	SKALOWALNOŚĆ
	Oprogramowanie musi być dostarczone wraz z wszystkimi komponentami koniecznymi do jego uruchomienia, działania i bezterminowego korzystania z wszystkich wymienionych
	i opisanych w tym dokumencie funkcjonalności.
	W przypadku istnienia ograniczenia licencyjnego na ilość agentów Zamawiający wymaga licencji umożliwiającej ciągłe zbieranie danych z minimum 20000 agentów.
	Oprogramowanie musi posiadać funkcjonalność skalowania infrastruktury co w momencie zakupu dodatkowych licencji pozwoli na obsługę większej porcji ruchu. W systemie musi istnieć mechanizm dodawania nowych węzłów pozwalających na zwiększenie wydajności dziennika.
	Oprogramowanie musi posiadać opcję pracy klastrowej w celu zabezpieczenia danych przed utratą w momencie uszkodzenia jednego węzła.
9	ZABEZPIECZENIE DOSTĘPU
	Dostęp do oprogramowania musi być zabezpieczony hasłem..
	Oprogramowanie musi pozwalać na zabezpieczenie dostępu z poziomu operatora i użytkownika oprogramowania za pomocą protokołu HTTPS.
	Oprogramowanie musi zapewniać kontrolę dostępu do gromadzonych danych bazującą na metodzie RBAC (Role Based Access Control).

10 Instalacja i konfiguracja dostarczonej infrastruktury i oprogramowania.

Dla rozwiązania, na które składa się infrastruktura opisana w punkcie 7. Opis techniczny posiadanej infrastruktury oraz infrastruktura dostarczana w ramach przedmiotu zamówienia wyspecyfikowana w punkcie 9. Dostawa infrastruktury i oprogramowania, Wykonawca zobowiązany jest m.in. do:

1. Przygotowania „Planu instalacji i konfiguracji" i uzyskania jego akceptacji przez Zamawiającego – dokument musi zawierać szczegółowe informacje nt. sposobu implementacji wraz z harmonogramem realizacji poszczególnych czynności. Wykonawca przygotuje i przedstawi do akceptacji Zamawiającego „Plan instalacji i konfiguracji" najpóźniej w terminie 30 dni od dnia podpisania Umowy. Wykonawca zobowiązany będzie do utrzymania aktualności opracowanego dokumentu w toku bieżącej realizacji przedmiotu umowy. Wykonawca dopełni wszystkich starań aby zapewnić realizację usługi instalacji i konfiguracji w jak najkrótszym czasie. Każda planowana niedostępność elementów infrastruktury i usług musi być przedstawiona w planie instalacji i konfiguracji, i musi uzyskać akceptację Zamawiającego.
2. Instalacji i konfiguracji zgodnie z zaakceptowanym przez Zamawiającego „Planem instalacji i konfiguracji". Sprzęt musi zostać zainstalowany we wskazanym przez Zamawiającego miejscu w serwerowni – wskazanym w „Planie instalacji i konfiguracji", w uzgodnionej lokalizacji, tak aby zapewnić maksymalną możliwą ciągłość działania poszczególnych warstw infrastruktury.
3. Migracji danych z obecnie posiadanego przez Zamawiającego środowiska. W ramach zadania Wykonawca zobowiązany jest do przeprowadzenia wszelkich prac związanych z konfiguracją oraz migracją danych zgromadzonych w obecnych magazynach danych, z zachowaniem maksymalnej możliwej dostępności Usług i Systemów oraz spójności danych. Należy również przeprowadzić rekonfigurację obecnego środowiska tak aby w maksymalnym stopniu ograniczyć konieczność zmian konfiguracji Systemów i Usług.

   Migracji podlegać będą w szczególności:

   - Bazy danych,
   - Maszyny wirtualne,
   - Zasoby plikowe,
   - Monitorowane obiekty (dla środowiska monitoringu),

4. W przypadku konieczności wykorzystania dodatkowych licencji lub oprogramowania Wykonawca zobowiązany jest do zapewnienia ich na czas trwania migracji danych, instalacji i konfiguracji.
5. Implementacji połączenia infrastruktury z obu pomieszczeń serwerowni do koncepcji wspólnej chmury obliczeniowej, z zachowaniem wymaganych parametrów RTO, RPO opisanych w rozdziale 8 Ogólna koncepcja docelowego rozwiązania.
6. Sporządzenia kompletu dokumentacji powykonawczych dla poszczególnych elementów infrastruktury i oprogramowania zgodnie z rozdziałem 17. Dokumentacja.
7. Przeprowadzenia testów akceptacyjnych. Testy będą prowadzone przez Zamawiającego, przy wsparciu Wykonawcy.

   Etap ten przewidziany jest również na usuwanie przez Wykonawcę wszelkich nieprawidłowości wykrytych podczas testów oraz niezgodności funkcjonalnych wobec „Planu instalacji i konfiguracji". Przeprowadzenie testów z wynikiem pozytywnym jest jednym z warunków odbioru wybranej pozycji z „Planu instalacji i konfiguracji".

Jeżeli w którejkolwiek z warstw obecnie posiadanego przez Zamawiającego rozwiązania wymagany będzie demontaż sprzętu, czynność ta leży w obowiązku Wykonawcy. Czynność deinstalacji należy przeprowadzić w taki sposób aby Zamawiający nie stracił posiadanej gwarancji na posiadany sprzęt.

Wykonawca dostarczy szczegółowy wykaz dostarczanego sprzętu oraz licencji i zasili tymi danymi bazę konfiguracji Zamawiającego.

Szczególne wymagania dla wybranych elementów infrastruktury i oprogramowania, zostały opisane poniżej:

10.1 Obudowy blade (klatki)

- Podłączenie do sieci LAN, SAN.

10.2 Serwery

- Instalacja 6 szt. serwerów w posiadanej przez Zamawiającego klatce blade wraz z analogiczną konfiguracją jak pozostałe serwery w klatce. Instalacja środowiska wirtualizacji.
- Instalacja 20 szt. serwerów w dostarczanych klatkach blade wraz z konfiguracją. Instalacja środowiska wirtualizacji.

10.3 Macierze blokowe

10.3.1 Macierz blokowa typ A

- Podłączenie do sieci SAN.
- Skonfigurowanie wymaganych zasobów dyskowych dla serwerów.
- Skonfigurowanie replikacji macierzy za pośrednictwem rozwiązania do wirtualizacji macierzy.

10.3.2 Macierz blokowa typ B

- Podłączenie do sieci SAN.
- Skonfigurowanie wymaganych zasobów dyskowych dla serwerów.
- Skonfigurowanie replikacji macierzy do macierzy blokowej typ C za pośrednictwem rozwiązania do wirtualizacji macierzy.

10.3.3 Macierz blokowa typ C

- Podłączenie do sieci SAN.
- Skonfigurowanie wymaganych zasobów dyskowych dla serwerów.

10.4 Rozwiązanie NAS

- Rozwiązanie NAS typ A ma pracować jako główne rozwiązanie. Dane z rozwiązania NAS typ A mają być replikowane synchronicznie do rozwiązania NAS typ B. Dane z rozwiązania NAS typ B mają być replikowane asynchronicznie do rozwiązania NAS typ C i zapewnić kopie przyrostowe danych, tzn. zmiany danych w rozwiązaniu NAS typ B nie powinny nadpisywać wcześniej zreplikowanych danych w rozwiązania NAS typ C.
- W ramach migracji danych z dotychczasowego rozwiązania typu NAS należy zachować dotychczasowe prawa dostępu do plików dla użytkowników/grup.
- Migracji podlega ok. 420TB danych plikowych zgromadzonych w obecnie używanym przez Zamawiającego rozwiązaniu NAS.

10.5 Switch SAN

- Połączenie z posiadaną przez Zamawiającego siecią SAN.
- Skonfigurowanie połączeń dla dostarczanych urządzeń, wymagających sieci SAN, np. serwery, macierze.

10.6 Oprogramowanie baz danych

Migracja obecnie utrzymywanych przez Zamawiającego baz danych na dostarczone w ramach niniejszego postępowania serwery (4 serwery RACK typ A) i macierzy blokowej (Macierz blokowa typ B). Zamawiający nie wymaga zmiany lub aktualizacji silnika bazy danych, jedynie przeniesienia baz danych na nowy sprzęt dostarczany w ramach niniejszego postępowania. Wielkość baz danych podlegających migracji wynosi ok. 90TB, w przeszło 60 instancjach baz danych.

10.7 Oprogramowanie do wirtualizacji serwerów

Oprogramowanie należy zainstalować na dostarczonych serwerach blade. Skonfigurować połączenia z posiadanym przez Zamawiającego środowiskiem wirtualizacji w celu realizacji koncepcji prywatnej chmury obliczeniowej.

10.8 Oprogramowanie do wirtualizacji sieci

W ramach implementacji dostarczonego rozwiązania należy przeprowadzić segmentację sieci LAN. W szczególności odseparowanie warstw: baz danych, NAS, backup.; środowisk produkcyjnych i testowych oraz maszyn wirtualnych w ramach projektów.

Powyższą rekonfiguracje należy przeprowadzić zarówno w obecnej infrastrukturze i w dostarczanej w ramach niniejszego Postępowania. W ramach procesu segmentacji należy uwzględnić wszystkie warstwy wymagające dostosowania.

10.9 Oprogramowanie do ochrony antywirusowej

Instalacja na nowych serwerach blade podłączanych do środowiska wirtualizacji i połączenie z istniejącą konsolą zarządzania.

10.10 Oprogramowanie do wykonywania kopii zapasowej

- Instalacja środowiska.
- Włączenie do wykonywania kopii zapasowej maszyn wirtualnych na 20 dostarczonych serwerów blade.
- Jako miejsce składowania kopii bezpieczeństwa należy wykorzystać posiadane przez Zamawiającego EMC DataDomain DD2500.

10.11 Oprogramowanie ITSM

Wykonawca zobowiązany jest m.in. do przeprowadzenia następujących czynności:

- instalacja oprogramowania dla środowiska produkcyjnego i testowego,
- weryfikacja i przegląd obecnie wdrożonych procesów ITIL,
- analiza wymagań i konsultacje merytoryczne,
- implementacja obecnie funkcjonujących procesów, kont użytkowników, grup, kolejek, CMDB.

10.12 Urządzenia sieciowe

Do Wykonawcy należy przygotowanie projektu sieci LAN z uwzględnieniem:

- przełączników w koncepcji SPINE – LEAF oraz Top of Rack,
- urządzeń routingu,
- urządzeń bezpieczeństwa,
- segmentacji sieci z uwzględnieniem konfiguracji w ramach oprogramowania do wirtualizacji sieci,
- dobrych praktyk oraz zasad bezpieczeństwa;

Na podstawie zaakceptowanego przez Zamawiającego projektu, należy przeprowadzić rekonfigurację obecnej infrastruktury sieciowej oraz wdrożyć nowe elementy infrastruktury.

10.13 Narzędzie wspierające

10.13.1 Narzędzie do monitorowania infrastruktury

Wykonawca zobowiązany jest m.in. do przeprowadzenia następujących czynności:

- instalacja oprogramowania dla środowiska produkcyjnego i testowego,
- weryfikacja i przegląd obecnie monitorowanych obiektów,
- analiza wymagań i konsultacje merytoryczne,
- migracja obecnie monitorowanych obiektów do nowego środowiska monitoringu,
- konfiguracja monitorowania nowej infrastruktury sprzętowej, wirtualnej, sieciowej oraz systemowej.

10.13.2 System analizy ruchu sieciowego i wykrywania anomalii

Wykonawca zobowiązany jest m.in. do przeprowadzenia następujących czynności:

- instalacja oprogramowania dla środowiska produkcyjnego wraz z podłączeniem źródeł danych.

10.13.3 Narzędzia do przechowywania, wizualizacji, wyszukiwania i analizy danych

Wykonawca zobowiązany jest m.in. do przeprowadzenia następujących czynności:

- instalacja oprogramowania dla środowiska produkcyjnego wraz z podłączeniem źródeł danych.

10.14 Szyna Usług

Migracja obecnie utrzymywanych przez Zamawiającego środowiska szyny usług SOA Oracle Service Bus na dostarczone w ramach niniejszego postępowania serwery RACK typ B i macierzy blokowej (Macierz blokowa typ C).

11 Utrzymanie

W okresie obowiązywanie umowy Wykonawca będzie zobowiązany m.in. do pełnienia roli podmiotu realizującego utrzymanie infrastruktury sprzętowo-programowej opisanej w punkcie 7. Opis techniczny posiadanej infrastruktury i punkcie 9. Dostawa infrastruktury i oprogramowania. Wykonawca powinien uwzględnić dodatkowo możliwość zaistnienia zmian w infrastrukturze posiadanej obecnie i w przyszłości przez Zamawiającego, w ramach realizacji innych działań wynikłych poza niniejszym przedmiotem zamówienia w trakcie trwania usługi utrzymania.

Utrzymanie systemu przez Wykonawcę będzie przebiegało etapami. Podział na etapy wynika m.in. z realizacją prac przy rozbudowie systemów GUGiK w ramach projektów CAPAP, ZSIN-Faza II i K-GESUT.

Wyróżnia się następujące etapy:

- Przejęcie utrzymania obecnie infrastruktury i systemów Zamawiającego
- Etap dostawy i konfiguracji nowej infrastruktury
- Etap wdrożenia produktów projektów CAPAP, K-GESUT, ZSIN Faza II
- Etap utrzymania po zakończeniu etapu dostawy i konfiguracji

11.1 Utrzymanie obecnej infrastruktury

Obecnie posiadana przez Zamawiającego infrastruktura utrzymywana była przez firmę zewnętrzną w okresie do 31 grudnia 2016.

Zakres obecnie realizowanych prac przez wyżej wymienioną firmę zewnętrzną to :

- OBSZAR SERWISU
    - Funkcja Service Desk (Centrum Obsługi Użytkowników)
    - Zarządzanie realizacją wniosków o usługi (zarządzanie zleceniami standardowymi)
    - Zarządzanie Incydentami
    - Zarządzanie Problemami
- OBSZAR UTRZYMANIA
    - Zarządzanie poziomem Usług
    - Zarządzanie katalogiem usług
    - Zarządzanie dostępnością i pojemnością zasobów
    - Zarządzanie zmianami w usługach
    - Zarządzanie konfiguracją

  - Operacyjne utrzymanie i eksploatacja infrastruktury
  - Monitoring infrastruktury i zarządzanie zdarzeniami
  - Zarządzania architekturą
  - Zarządzanie bezpieczeństwem informacji i uprawnieniami dostępu
  - Utrzymanie narzędzi ITSM
- UTRZYMANIE DOKUMENTACJI PROCESÓW UTRZYMANIA I SERWISU

Zakres prac realizowanych przez zespół zamawiającego zgodnie z metodyką ITIL 2011.

11.2 Przejęcie utrzymania obecnie posiadanej przez Zamawiającego infrastruktury i systemów

W pierwszym etapie utrzymania Wykonawca zobowiązany będzie do przejęcia usługi utrzymania po zakończeniu świadczenia usługi przez dotychczasowy podmiot. W okresie 2 miesięcy od daty rozpoczęcia świadczenia usługi przez Wykonawcę, Zamawiający nie będzie naliczał kar za niedotrzymanie warunków gwarantowanego poziomu świadczenia usług - SLA. W tym czasie Wykonawca powinien nabyć niezbędne doświadczenie tak aby po tym okresie świadczyć usługi utrzymania zgodnie z warunkami opisanymi w punkcie 14. Parametry obowiązujące Wykonawcę.

Wykonawca w porozumieniu z Zamawiającym wykona analizę istniejącej infrastruktury, której celem będzie :

- Zdefiniowanie przydatności poszczególnych komponentów w docelowym rozwiązaniu
- Zdefiniowanie parametrów jakościowych poszczególnych komponentów
- Zdefiniowanie przeznaczenia dla poszczególnych komponentów
- Określenie sposobu wykorzystania poszczególnych komponentów w docelowym rozwiązaniu
- Harmonogram realizacji

Wyżej wymieniona analiza stanowić będzie podstawę do przygotowania planu instalacji i konfiguracji.

Usługa utrzymania na tym etapie będzie dotyczyła infrastruktury sprzętowo-programowej opisanej w punkcie 7. Opis techniczny posiadanej infrastruktury.

11.3 Etap dostawy i konfiguracji nowej infrastruktury

W kolejnym etapie Wykonawca zobowiązany będzie do świadczenia usługi utrzymania w zakresie dotychczasowej infrastruktury, z uwzględnieniem zmian związanych z przystosowaniem tejże infrastruktury do funkcjonowania w rozwiązaniu docelowym, dopuszczonych przez Zamawiającego

oraz infrastruktury dostarczanej w ramach niniejszego postępowania opisanej funkcjonalnie w rozdziale 9. Dostawa infrastruktury i oprogramowania.

Etap rozpoczyna się po podpisaniu umowy. Termin instalacji i konfiguracji uzależniony jest od terminu realizacji prac dostosowania pomieszczeń serwerowni. Zamawiający przewiduje zakończenie przystosowania pomieszczeń serwerowni na I kwartał 2018.

W zakresie usług świadczonych przez Wykonawcę będzie m.in. instalacja i konfiguracja dostarczanej infrastruktury zgodnie z punktem 10. Instalacja i konfiguracja dostarczonej infrastruktury i oprogramowania. Realizacja prac ma być realizowana zgodnie z przyjętymi procedurami utrzymaniowymi.

Wykonawca musi uwzględnić proces migracji danych, zgodnie z punktem 10. Instalacja i konfiguracja dostarczonej infrastruktury i oprogramowania.

W trakcie instalacji i modyfikacji Wykonawca zobowiązany jest zapewnić jak najkrótszy okres niedostępności systemu.

11.4 Etap wdrożenia produktów projektów CAPAP, K-GESUT, ZSIN Faza II

Równolegle z realizacją niniejszego przedmiotu umowy Zamawiający przewiduje wyłonienie podmiotu, który będzie realizował usługę rozbudowy i rozwoju systemów SIG.

Wykonawca niniejszego przedmiotu umowy musi być gotowy do współpracy z Wykonawcą rozbudowy i rozwoju systemów SIG. Wśród standardowych zadań realizowanych przez Wykonawcę mogą pojawić się:

- Rekonfiguracja szyny usług (zgodnie dokumentacją zmiany)
- Przygotowanie środowiska testowego oraz produkcyjnego we wszystkich warstwach infrastruktury (zgodnie dokumentacją zmiany)
- Wdrożenie paczki instalacyjnej na środowisku produkcyjnym (zgodnie z dokumentacją zmiany)

Zamawiający przewiduje, że rozbudowa i rozwój systemów SIG będzie się odbywać na wszystkich etapach realizacji utrzymania tj. przed wdrożeniem docelowej infrastruktury, podczas wdrożenia oraz po zakończeniu dostawy i konfiguracji.

11.5 Etap utrzymania po zakończeniu etapu dostawy i konfiguracji

Po zakończeniu wdrożenia docelowego rozwiązania sprzętowo-programowego (w tym po przeniesieniu danych magazynowanych w zasobie geodezyjnym) Wykonawca będzie świadczył usługę utrzymania całej infrastruktury.

Wykonawca uwzględni możliwość uruchomienia w infrastrukturze Zamawiającego nowych projektów, w tym musi przewidzieć możliwość świadczenia usług Utrzymania, zgodnych z zakresem opisanym w przedmiotowym dokumencie, dla nowych projektów realizowanych przez Zamawiającego oraz podmioty współpracujące z Zamawiającym.

11.6 Dokumentacja utrzymywanych rozwiązań

W ramach utrzymania należy przewidzieć konieczność aktualizacji lub wytworzenia dokumentacji utrzymaniowej.

Zakres dokumentacji Zamawiającego obejmuje m.in.:

- Dokumentacja utrzymaniowa:
  - Definicje procesów
  - Funkcja Service Desk (Centrum Obsługi Użytkowników)
  - Zarządzanie realizacją wniosków o usługi (zarządzanie zleceniami standardowymi)
  - Zarządzanie incydentami
  - Zarządzanie problemami
  - Zarządzanie poziomem usług
  - Zarządzanie katalogiem usług
  - Zarządzanie dostępnością i pojemnością zasobów
  - Zarządzanie zmianami w usługach
  - Zarządzanie konfiguracją
  - Zarządzanie ciągłością działania
  - Operacyjne utrzymanie i eksploatacja infrastruktury
  - Monitoring infrastruktury i zarządzanie zdarzeniami
  - Zarządzania architekturą
  - Zarządzanie bezpieczeństwem informacji i uprawnieniami dostępu
  - Utrzymanie narzędzi ITSM
- Raporty miesięczne
  - Dokumentacja procesów ITIL

  - Dokumentacja Service Desk
  - Dokumentacja zarządzania dostępnością, pojemnością, zasobami
  - Dokumentacja zarządzania konfiguracją
  - Dokumentacja zarządzania zmianami
  - Miesięczny raport z utrzymania
- Dokumentacja procesów
  - Procedury, instrukcje dot. Standardowych modeli incydentów
  - Dokumentacja obejść i rozwiązań docelowych
  - Rejestr inicjatyw doskonalących, usprawnień
  - Katalogi usług
  - Plan dostępności i pojemności
  - Raporty z monitoringu dostępności i pojemności
  - Raport trendów dostępności i pojemności usług i infrastruktury
  - Dziennik administratora
  - Raporty dla obszaru oprogramowania standardowego
  - Plany wprowadzania i wycofywania zmian
  - Dokumentacja projektów zmian
  - Opinie, analizy zmian
  - Raporty, protokoły z działań w zakresie zarządzania zmianami i ich wdrażaniem
  - Plany zarządzania konfiguracją
  - Strategia ciągłości IT
  - Plany ciągłości
  - Raporty z testów i przeglądów planów ciągłości
  - Procedury administrowania i utrzymania
  - Raport, protokół z realizowanej czynności administracyjnej
  - Koncepcja monitorowania
  - Raporty cząstkowe z monitoringu
  - Polityka bezpieczeństwa
  - Procedury i instrukcje bezpieczeństwa
  - Dokument analizy ryzyka dla infrastruktury IT
  - Dokumentacja konfiguracji narzędzi ITSM
  - Szablon procedury i instrukcji utrzymaniowej
- Dokumentacja do systemów:
  - Dokumentacja powykonawcza
  - Dokumentacja utrzymaniowa

- Dokumentacja do infrastruktury:
    - Architektura rozwiązania
    - Dokumentacja utrzymaniowa
    - Dokumentacja techniczna infrastruktury
    - Raport z utrzymania
    - Analiza ryzyka
    - Instrukcje stanowiskowe.

11.7 Przekazanie utrzymania infrastruktury i systemów

W ostatnim etapie utrzymania Wykonawca zobowiązany będzie do przekazania usługi utrzymania. W okresie 3 miesięcy przed data zakończenia świadczenia usługi Wykonawca przygotuje „Plan przekazania utrzymania infrastruktury". Plan musi zostać uzgodniony i zaakceptowany przez Zamawiającego.

Plan przekazania utrzymania infrastruktury musi zawierać m.in. następujące informacje:

- Informacje o stanie poszczególnych warstw infrastruktury i systemów
- Sposób, terminy przekazania i zmiany haseł administracyjnych oraz wszystkich dostępów do infrastruktury
- Harmonogram przekazania infrastruktury

12 Zakres prac Utrzymaniowych

Poniższe zadania będą realizowane z wykorzystaniem istniejących procedur utrzymaniowych i eksploatacyjnych Zamawiającego lub procedur przygotowanych przez Wykonawcę, a zaakceptowanych przez Zamawiającego oraz:

- poprzez wdrożone, będące w posiadaniu Zamawiającego narzędzia ITSM m.in. : HP Service Manager, HP Business Service Management, Nagios, Centreon i Nagvis, OpenAudit - do czasu wdrożenia nowych narzędzi ITSM;
- poprzez nowe narzędzia ITSM - po ich wdrożeniu.

12.1 Obszar serwisu

W ramach odpowiedzialności za obszar serwisu Wykonawca jest zobowiązany do realizacji kompleksowych działań związanych z identyfikacją, rejestracją, kategoryzacją, priorytetyzacją, obsługą, rozwiązywaniem oraz eskalacją do podmiotów właściwych dla obsługi, rozwiązania, dokumentowaniem rozwiązań oraz zamykaniem wszystkich zgłoszeń tj. zmian, incydentów i problemów. W ramach działań Wykonawca zobowiązany jest do organizacji funkcji Service-Desk, stanowiącej pierwszą linię wsparcia i diagnozy dla wszystkich zgłoszeń oraz wiodącą rolę uczestniczącą w procesach obszaru wsparcia opisanych w kolejnych podrozdziałach.

12.1.1 Funkcja Service Desk (Centrum Obsługi Użytkowników)

Funkcja Service Desk stanowi pojedynczy punkt kontaktu użytkowników SIG z obszarem IT we wszystkich sprawach związanych z użytkowaniem usług oraz infrastruktury. Service Desk jest pośrednikiem pomiędzy użytkownikami, zespołami utrzymaniowymi, wykonawcami systemów oraz wykonawcami realizującymi umowy serwisowe i asystę techniczną). Service Desk jest odpowiedzialny za przyjmowanie zgłoszeń od użytkowników i kontrolującym ich rozwiązanie. Głównym zadaniem Service Desk jest wsparcie wszystkich użytkowników SIG (zarówno wewnętrznych w GUGiK i CODGIK jak i zewnętrznych – klientów GUGiK) w zakresie rozwiązywania ich zgłoszeń.

Do klientów GUGiK należą w szczególności:

- służby ratunkowe instytucje Państwowe, jako partnerzy korzystający z rozwiązania Geoportal, np. Policja, Państwowa Straż Pożarna, Starostwa Powiatowe, WCPR.

- pozostali użytkownicy, np. osoby prywatne, firmy korzystające z usług rozwiązania Geoportal.

Obecna skala zgłoszeń wynosi ok. 3000 zgłoszeń rocznie i ok. 2000 zmian utrzymaniowych.

Zamawiający przewiduje zwiększenie liczby zgłoszeń w okresie trwania umowy o około 50%.

W ramach swoich zadań Service Desk będzie zarządzać zmianami, incydentami i problemami.

Do podstawowych zadań realizowanych przez Service Desk zalicza się:

1. przyjmowanie i rejestrowanie zgłoszeń z wykorzystaniem wszystkich dostępnych kanałów komunikacji,
2. udzielanie bezpośredniego wsparcia w zakresie obsługiwanych i eksploatowanych systemów składających się na SIG, poprzez obsługę zgłoszeń,
3. kierowanie zgłoszeń do odpowiednich zespołów merytorycznych złożonych z pracowników GUGiK, CODGiK, pracowników Wykonawcy oraz podmiotów trzecich,
4. rozwiązywanie zgłoszeń pozostających w kompetencjach Service Desk,
5. koordynacja procesu zamykania zgłoszeń,
6. monitorowanie postępów prac nad zmianami, incydentami i problemami, a także eskalacja zgodnie z ustalonymi poziomami świadczenia usług,
7. przygotowywanie wytycznych i zaleceń dla kolejnych linii wsparcia,
8. koordynacja i przygotowywanie raportów miesięcznych oraz raportów na żądanie,
9. aktualizacja dokumentacji (procedur, sprawozdań, raportów oraz analiz) w ramach obszaru, w tym uzupełnianie Bazy Wiedzy, Bazy Konfiguracji, Katalogu Usług Infrastrukturalnych oraz Katalogu Usług Biznesowych,
10. monitorowanie parametrów usług świadczonych przez SIG, w przypadku niedotrzymania parametrów usług zgłaszanie incydentów. Wykonawca jest zobowiązany zgłaszać incydenty zgodnie z parametrami dla Czasu reakcji na incydent określonymi w poz. 1 tabeli Tabela 16 w rozdziale 14.2.1. Wartości parametrów.

Wykonawca musi zapewnić dostępność:

- co najmniej 1 specjalisty pełniącego rolę Operatora Service Desk przez 7 dni w tygodniu, 24 godziny na dobę,
- w godzinach roboczych – co najmniej 1 specjalistę pełniącego rolę Koordynatora Service Desk.

12.1.1.1 Kanały komunikacji z Service Desk

W celu zapewnienia wysokiego poziomu obsługi zgłoszeń i napotkanych błędów w funkcjonowaniu SIG zgłoszenia są przekazywane przez użytkowników poprzez 3 kanały komunikacyjne:

- za pośrednictwem Systemu Zgłoszeń,
- telefonicznie,
- za pośrednictwem poczty elektronicznej.

12.1.2 Zarządzanie realizacją wniosków o usługi

Proces Zarządzania realizacją wniosków o usługi jest odpowiedzialny za zarządzanie cyklem życia dla wszystkich Wniosków o usługi, tj. umożliwienie użytkownikom wnioskowania o standardowe usługi i otrzymywania tych usług. Standardowe usługi stanowią prośby użytkowników o informacje, zmiany standardowe lub dostęp do świadczonych usług.

W ramach procesu, Wykonawca będzie odpowiedzialny za realizację następujących aktywności:

1. Przyjmowanie i rejestrowanie wniosków o usługi.
2. Kategoryzacja i priorytetyzacja wniosków o usługi.
3. Obsługa zgłoszeń / wniosków o usługi pozostających w kompetencjach Wykonawcy.
4. Eskalacja / kierowanie obsługi wniosków o usługi do właściwych jednostek / podmiotów dla wniosków, które pozostają poza kompetencjami Wykonawcy.
5. Wsparcie pozostałych jednostek / podmiotów w obsłudze wniosków o usługi w przypadku zaistnienia takiego zapotrzebowania.
6. Bieżące informowanie Zamawiającego o postępie w obsłudze wniosków o usługi oraz raportowanie ich obsługi.
7. Potwierdzanie ze zgłaszającym możliwości zamknięcia wniosku o usługę oraz zamknięcie zgłoszenia.
8. Dokumentowanie zgłoszeń i ich obsługi w narzędziach wspierających proces (narzędzia ITSM).

W ramach realizacji działań procesu Wykonawca jest zobowiązany do bieżącego utrzymania minimum następujących dokumentów:

Tabela 1. Dokumentacja zarządzania realizacją wniosków o usługi

Lp.	Nazwa	Opis / Ramowy zakres	Terminy przekazania
1.	Definicja procesu	Dokument opisu procesu obejmujący co najmniej jego cel, politykę, diagram z przebiegiem, opis kroków, opis ról i odpowiedzialności (wraz z tabelą RACI), miary, produkty, kluczowe procedury i instrukcje	Inicjalnie wraz z raportem za 1-wszy m-c utrzymania oraz każdorazowo w terminie 14 dni od modyfikacji
2.	Raport z utrzymania	Dokument cyklicznego raportu w zakresie przynależnym dla procesu, zgodnie z rozdziałem 15.2	Comiesięcznie, zgodnie z cyklem raportowania

Ponadto efektem działania procesu będzie bieżące aktualizowanie informacji w narzędziach ITSM wspierających działanie procesu.

12.2 Zarządzanie Incydentami

Celem procesu Zarządzania Incydentami jest minimalizowanie negatywnego wpływu przerw w świadczeniu usług lub obniżenia jakości usług (incydentów) na działania klientów korzystających z tych usług oraz jak najszybsze przywracanie funkcjonowania usług zachwianych przez incydenty. Ponieważ część ze zgłaszanych incydentów będzie miała swoje źródło w infrastrukturze utrzymywanej przez Wykonawcę, będzie on realizował wsparcie obsługi incydentów w obszarze, który znajduje się w zakresie jego odpowiedzialności.

W ramach procesu, Wykonawca będzie odpowiedzialny za realizację następujących aktywności:

1. Identyfikacja i rejestrowanie incydentów.
2. Kategoryzacja i priorytetyzacja incydentów.
3. Opracowywanie rozwiązań dla incydentów związanych z obszarem jego odpowiedzialności.
4. Eskalowanie obsługi incydentów do pozostałych linii wsparcia dla incydentów dotyczących obszarów systemu pozostających poza bezpośrednią kontrolą Wykonawcy.
5. Wsparcie pozostałych linii wsparcia w badaniu i diagnozie incydentów dotyczących infrastruktury.
6. Dokumentowanie opracowywanych rozwiązań dla incydentów oraz ich obsługi w narzędziach wspierających proces (narzędzia ITSM).
7. Opracowywania standardowych modeli obsługi incydentów dla incydentów, które wystąpiły minimum 3 razy.
8. Rejestracja problemów w celu identyfikacji i usunięcia przyczyn wystąpienia incydentów.
9. Przywracanie funkcjonalności systemu zachwianej przez incydenty poprzez wprowadzanie na środowiska testowe i produkcyjne rozwiązań dla incydentów.
10. Bieżące informowanie Zamawiającego o postępie w obsłudze incydentów, raportowanie obsługi incydentów.
11. Potwierdzanie ze zgłaszającym możliwości zamknięcia incydentu oraz zamknięcia zgłoszenia.

12.2.1 Produkty procesu

W ramach realizacji działań procesu Wykonawca jest zobowiązany do bieżącego utrzymania minimum następujących dokumentów:

Tabela 2. Dokumentacja zarządzania Incydentami

Lp.	Nazwa	Opis / Ramowy zakres	Terminy przekazania
1.	Definicja procesu	Dokument opisu procesu obejmujący co najmniej jego cel, politykę, wyzwalacze, diagram z przebiegiem, opis kroków, opis ról i odpowiedzialności (wraz z tabelą	Inicjalnie wraz z raportem za 1-wszy m-c utrzymania oraz

		RACI), miary, produkty, kluczowe procedury i instrukcje	każdorazowo terminie 14 dni od modyfikacji
2.	Raport z utrzymania	Dokument cyklicznego raportu w zakresie przynależnym dla procesu, zgodnie z rozdziałem 15.2	Comiesięcznie, zgodnie z cyklem raportowania
3.	Procedury / instrukcje dot. Standardowych modeli incydentów	Dokument instrukcji / procedury obejmujący co najmniej symptomy / wyzwalacze, opis przebiegu (czynności), opis odpowiedzialności, oczekiwany efekt. Dokument będzie umieszczany w bazie wiedzy	Zgodnie z tabelą w rozdziale 14.2

Ponadto efektem działania procesu będzie bieżące aktualizowanie informacji w narzędziach ITSM wspierających działanie procesu.

12.3 Zarządzanie Problemami

Zarządzanie problemami jest odpowiedzialne za poszukiwanie przyczyn występowania incydentów, opracowywanie rozwiązań tymczasowych i docelowych zmierzających do usuwania źródłowych przyczyn powstawania incydentów oraz proaktywne zarządzanie problemami zmierzające do redukcji liczby incydentów pojawiających się w przyszłości.

W ramach swojego obszaru odpowiedzialności Wykonawca będzie realizował zadania związane z całościową obsługą problemów dotyczących obszaru infrastrukturalnego utrzymywanych systemów.

W ramach procesu Wykonawca będzie odpowiedzialny za realizację następujących aktywności:

1. Rejestrowanie zidentyfikowanych problemów w zakresie infrastruktury podlegającej jego utrzymaniu.
2. Kategoryzowanie i priorytetyzowanie problemów.
3. Wykonywanie badania i diagnozy problemów.
4. Dokumentowanie przyczyn źródłowych problemów.
5. Wypracowywanie i dokumentowanie obejść dla problemów, wprowadzanie obejść na środowisko testowe i produkcyjne lub inicjowanie wprowadzania opracowanych obejść na środowisko testowe i produkcyjne poprzez przygotowywanie wniosków o zmiany jeśli wymagają one formalnego uruchomienia procesu zarządzania zmianą.
6. Wypracowywanie i dokumentowanie rozwiązań dla problemów, inicjowanie wprowadzania opracowanych rozwiązań na środowisko testowe i produkcyjne poprzez przygotowywanie wniosków o zmiany dla przygotowanych rozwiązań.
7. Bieżące informowanie Zamawiającego o postępie w obsłudze problemów, raportowanie obsługi problemów.
8. Zamykanie rekordów problemów (w tym potwierdzanie zamknięcia z Zamawiającym).

9. Prowadzenie działań proaktywnych, mających na celu zapobieganie występowania Problemów poprzez identyfikację i analizę często występujących Incydentów o podobnych symptomach, względnie pojedynczych Incydentów o dużym wpływie na systemy.
10. Rejestrowanie propozycji potencjalnych usprawnień zmierzających do zmniejszenia liczby pojawiających się w przyszłości incydentów i problemów dotyczących infrastruktury.
11. Utrzymywanie repozytorium problemów i znanych błędów, udostępnianie informacji zawartych w tych repozytoriach dla pozostałych linii wsparcia uczestniczących w diagnozie i rozwiązywaniu problemów.
12. Eskalowanie badania, diagnozy i rozwiązywania problemów do pozostałych linii wsparcia dla problemów, które dotyczą elementów systemów pozostających poza bezpośrednią odpowiedzialnością wykonawcy (np. błędy w aplikacjach, itd.)

12.3.1 Produkty procesu

W ramach realizacji działań procesu Wykonawca jest zobowiązany do bieżącego utrzymania minimum następujących dokumentów:

Tabela 3. Dokumentacja zarządzania Problemami

Lp.	Nazwa	Opis / Ramowy zakres	Terminy przekazania
1.	Definicja procesu	Dokument opisu procesu obejmujący co najmniej jego cel, politykę, wyzwalacze, diagram z przebiegiem, opis kroków, opis ról i odpowiedzialności (wraz z tabelą RACI), miary, produkty, kluczowe procedury i instrukcje	Inicjalnie wraz z raportem za 1-wszy m-c utrzymania oraz każdorazowo w terminie 14 dni od modyfikacji
2.	Raport z utrzymania	Dokument cyklicznego raportu w zakresie przynależnym dla procesu, zgodnie z rozdziałem 15.2	Comiesięcznie, zgodnie z cyklem raportowania
3.	Dokumentacja obejść i rozwiązań docelowych	Dokument instrukcji / procedury obejmujący co najmniej przyczynę źródłową, opis działań (czynności), opis odpowiedzialności, oczekiwany efekt. Dokument będzie umieszczany w bazie wiedzy.	Zgodnie z tabelą w rozdziale 14.2

Ponadto efektem działania procesu będzie bieżące aktualizowanie informacji w narzędziach ITSM wspierających działanie procesu.

12.4 Obszar utrzymania

12.4.1 Zarządzanie poziomem Usług

Proces zarządzania poziomem usług jest odpowiedzialny za ustalanie i dotrzymywanie wszystkich uzgodnionych z Zamawiającym parametrów jakościowych usług świadczonych w oparciu o utrzymywane systemy informatyczne. Wykonawca będzie odpowiedzialny za utrzymanie

parametrów dla świadczonych przez niego usług utrzymaniowych / technicznych (o charakterze wsparcia dla usług świadczonych za pomocą systemów ich klientom).

W ramach procesu Wykonawca będzie odpowiedzialny za realizację następujących aktywności:

1. Zapewnienie świadczenia usług technicznych wynikających z utrzymania infrastruktury Systemów oraz usług biznesowych na poziomach nie gorszych niż wskazane w rozdziale 14.1.
2. Raportowanie parametrów poziomu usług.

12.4.1.1 Produkty procesu

W ramach realizacji działań procesu Wykonawca jest zobowiązany do bieżącego utrzymania minimum następujących dokumentów:

Tabela 4. Dokumentacja zarządzania poziomem Usług

Lp.	Nazwa	Opis / Ramowy zakres	Terminy przekazania
1.	Definicja procesu	Dokument opisu procesu obejmujący co najmniej jego cel, politykę, wyzwalacze, diagram z przebiegiem, opis kroków, opis ról i odpowiedzialności (wraz z tabelą RACI), miary, produkty, kluczowe procedury i instrukcje	Inicjalnie wraz z raportem za 1-wszy m-c utrzymania oraz każdorazowo terminie 14 dni od modyfikacji
2.	Raport z utrzymania	Dokument cyklicznego raportu w zakresie przynależnym dla procesu, zgodnie z rozdziałem 15.2	Comiesięcznie, zgodnie z cyklem raportowania

Ponadto efektem działania procesu będzie bieżące aktualizowanie informacji w narzędziach ITSM wspierających działanie procesu.

12.4.2 Zarządzanie katalogiem usług

Proces Zarządzania katalogiem usług dba o spójność i zgodność ze stanem faktycznym zapisów w kartach usług w tym katalogu. W ramach procesu Wykonawca – dbając o spójność zapisów w obszarze usług wsparcia – będzie odpowiedzialny za utrzymywanie (w tym wprowadzanie nowych pojawiających się usług) katalogu usług wynikających z utrzymania infrastruktury SIG oraz utrzymania systemów. W ramach działania wykonawca będzie w szczególności aktualizował katalogi usług infrastrukturalnych oraz biznesowych, właściwe dla poszczególnych składowych SIG, z uwzględnieniem dekompozycji usług na poszczególne elementy i warstwy infrastruktury (najwyższą warstwę dla modelu logicznego infrastruktury mają stanowić usługi). Uzupełnianie i utrzymywanie informacji o usługach będzie realizowane w katalogach usług w narzędziach ITSM, przy czym:

- poprzez wdrożone, będące w posiadaniu Zamawiającego narzędzia ITSM m.in. : HP Service Manager, HP Business Service Management, Nagios, Centreon i Nagvis, OpenAudit - do czasu wdrożenia nowych narzędzi ITSM,
- poprzez nowe narzędzia ITSM - po ich wdrożeniu;

12.4.2.1 Produkty procesu

Tabela 5. Dokumentacja zarządzania katalogiem usług

Lp.	Nazwa	Opis / Ramowy zakres	Terminy przekazania
1.	Definicja procesu	Dokument opisu procesu obejmujący co najmniej jego cel, politykę, wyzwalacze, diagram z przebiegiem, opis kroków, opis ról i odpowiedzialności (wraz z tabelą RACI), miary, produkty, kluczowe procedury i instrukcje	Inicjalnie wraz z raportem za 1-wszy m-c utrzymania oraz każdorazowo terminie 14 dni od modyfikacji
2.	Raport z utrzymania	Dokument cyklicznego raportu w zakresie przynależnym dla procesu, zgodnie z rozdziałem 15.2	Comiesięcznie, zgodnie z cyklem raportowania
3.	Katalogi usług	Dokument katalogu usług zgodnie z obowiązującą strukturą	Zgodnie z tabelą w rozdziale 14.2

Ponadto efektem działania procesu będzie bieżące aktualizowanie informacji w narzędziach ITSM wspierających działanie procesu.

12.4.3 Zarządzanie dostępnością i pojemnością zasobów

Wykonawca będzie realizował zarządzanie dostępnością i pojemnością zasobów systemów poprzez monitorowanie, raportowanie, zapewnienie wymaganej dostępności i pojemności elementów SIG oraz przygotowywanie analiz i prognoz co do wykorzystania i ewentualnej rozbudowy zasobów utrzymywanych systemów.

W ramach procesu Wykonawca będzie odpowiedzialny za realizację następujących aktywności:

1. Bieżące monitorowanie i raportowanie dostępności i pojemności elementów infrastruktury systemów.
2. Utrzymywanie uzgodnionego z Zamawiającym poziomu dostępności i pojemności infrastruktury systemów poprzez:
    1) monitorowanie ryzyk i zagrożeń zachwiania uzgodnionego z Zamawiającym poziomu dostępności i pojemności elementów infrastruktury SIG,
    2) informowanie Zamawiającego o stanie infrastruktury potencjalnie mogącym prowadzić do niespełnienia parametrów dostępności i pojemności infrastruktury z wyprzedzeniem co najmniej 6-miesięcznym (punkt 5),

3) przygotowanie rekomendacji zmian i propozycji rozwiązań dla zapewnienia odpowiedniej pojemności / dostępności infrastruktury, w tym projektów uzasadnionej rozbudowy infrastruktury.

3. Prognozowanie obciążenia systemów oraz planowanie dostępności i pojemności elementów infrastruktury systemów, utrzymywanie planów dostępności i pojemności systemu, zarządzanie ryzykiem powstania niedostępności elementów infrastruktury systemowej, która może przełożyć się na niedostępność usług świadczonych w oparciu o te systemy.
4. Utrzymywanie aktualnej informacji o licencjach i warunkach wsparcia technicznego względem sprzętu i oprogramowania składających się na utrzymywane systemy.
5. Zgłaszanie zapotrzebowania na zakup sprzętu, licencji i aktualizacji niezbędnych ze względu na zapewnienie dostępności oraz pojemności elementów systemów(z wyprzedzeniem co najmniej 6-miesięcznym).
6. Wdrażanie na środowisko produkcyjne rozwiązań służących zapewnieniu wymaganej dostępności i pojemności infrastruktury systemów.
7. Podejmowanie działań mających na celu zapobieganie przeciążenia systemów.
8. Analiza danych pochodzących z monitorowania pod kątem trendów i odchyleń od przewidywań w celu prognozowania wykorzystania zasobów.
9. Badanie i diagnoza zidentyfikowanej niedostępności elementów infrastruktury systemów, planowanie działań zaradczych.
10. Strojenie elementów systemów w celu lepszego wykorzystania zasobów.

12.4.3.1 Produkty procesu

W ramach realizacji działań procesu Wykonawca jest zobowiązany do wytworzenia i bieżącego utrzymania minimum następujących dokumentów:

Tabela 6. Dokumentacja zarządzania dostępnością i pojemnością zasobów

Lp.	Nazwa	Opis / Ramowy zakres	Terminy przekazania
1.	Definicja procesu	Dokument opisu procesu obejmujący co najmniej jego cel, politykę, wyzwalacze, diagram z przebiegiem, opis kroków, opis ról i odpowiedzialności (wraz z tabelą RACI), miary, produkty, kluczowe procedury i instrukcje	Inicjalnie wraz z raportem za 1-wszy m-c utrzymania oraz każdorazowo w terminie 14 dni od modyfikacji
2.	Raport z utrzymania	Dokument cyklicznego raportu w zakresie przynależnym dla procesu, zgodnie z rozdziałem 15.2	Comiesięcznie, zgodnie z cyklem raportowania
3.	Plan dostępności i pojemności	Dokument obejmujący co najmniej zestawienie źródeł danych dla planu, opis założeń i rozważanych scenariuszy, zasięg planu (usługi i zasoby objęte planem), aktualne poziomy dostępności i pojemności dla usług i zasobów, prognozowane i wymagane poziomy dostępności i pojemności dla usług i zasobów (w oparciu o rozważane scenariusze, plany	Inicjalnie wraz z raportem za 1-wszy m-c utrzymania. Weryfikacja i aktualizacja kwartalna.

		rozwojowe, analizę trendów), planowane / postulowane działania, oszacowanie kosztów działań, rekomendacje realizacji działań.	
4.	Raporty z monitoringu dostępności i pojemności	Zestawienie wartości parametrów dostępności i pojemności podlegających monitorowaniu dla usług i elementów infrastruktury, zakres informacyjny zgodny z zakresem informacji w narzędziach monitorujących / narzędziach ITSM	Comiesięcznie, zgodnie z cyklem raportowania
5.	Raport trendów dostępności i pojemności usług i infrastruktury	Dokument obejmujący zestawienia trendów zmian dla parametrów dostępności i pojemności podlegających monitorowaniu dla usług i elementów infrastruktury oraz prognozy dla tych parametrów (w szczególności w zakresie wykorzystania zasobów, okresu działania w oparciu o obecne zasoby, potencjalnego zapotrzebowania na zakup)	Comiesięcznie, zgodnie z cyklem raportowania
6.	Dziennik administratora	Dokument dziennika administratora w zakresie przynależnym dla procesu (działania mające na celu zapobieganie przeciążeniu systemu, plany działań korygujących, strojenia elementów Systemu)	Comiesięcznie, zgodnie z cyklem raportowania
7.	Raporty dla obszaru oprogramowania standardowego	Dokument obejmuje co najmniej zestawienie licencji i wsparcia technicznego dla dostarczonych przez wykonawców elementów wraz z aktualnym okresem ważności oraz opcją wsparcia technicznego producenta w powiązaniu z opisem – która licencja jest niezbędna do realizacji której usługi) oraz sprzętu (usługi serwisu sprzętu).	Comiesięcznie, zgodnie z cyklem raportowania
8.	Rejestr inicjatyw doskonalących / usprawnień	Dokument obejmujący co najmniej datę zgłoszenia i zgłaszającego, klasę (wagę) inicjatywy, obszar (proces) genezę inicjatywy, opis rekomendowanego działania oraz status	Comiesięcznie, aktualizacja zgodnie z wewnętrznym harmonogramem realizacji działań proaktywnych w ramach zarządzania dostępnością i pojemnością

Ponadto efektem działania procesu będzie bieżące aktualizowanie informacji w narzędziach ITSM wspierających działanie procesu.

12.4.4 Zarządzanie zmianami w usługach

W okresie realizacji przedmiotu zamówienia na środowisku testowym i produkcyjnym będą pojawiać się zmiany w elementach SIG.

Wykonawcy systemów będą instalować/konfigurować systemy na środowiskach testowych pod nadzorem Wykonawcy.

Wykonawcy systemów będą instalować/konfigurować systemy na środowiskach produkcyjnych pod nadzorem Wykonawcy. Z działań tych wyłączone będą usługi infrastrukturalne (m.in. szyna usług, silnik bazy danych) utrzymywane przez Wykonawcę, dla których pełni on usługę konfiguracji, w oparciu o wniosek zgłaszany przez Wykonawcę systemów.

1. Wykonawca będzie zarządzał wprowadzaniem na środowisko testowe i produkcyjne zmian, obejmujących:
   1) zmiany eksploatacyjne / utrzymaniowe – związane z realizowanymi pracami o charakterze utrzymaniowo-eksploatacyjnym m.in. z modernizacją technologiczną infrastruktury, usuwaniem awarii oraz naprawą błędów w oprogramowaniu zainstalowanym na tej infrastrukturze (rozwiązania będą pochodziły np. z obszaru zarządzania problemami),
   2) zmiany rozwojowe – zmiany wynikające z realizowanego rozwoju systemu, w szczególności wprowadzania na środowisko testowe i produkcyjne elementów wskazywanych w rozdziale 12.1 (m.in. aplikacje, narzędzia, systemy).

2. Z punktu widzenia zapewnienia ciągłości działania Systemu niezbędne jest, aby wdrażanie zmian rozwojowych na środowisko produkcyjne odbywało się w skoordynowany sposób. Dlatego też niezbędne jest, aby wdrożenie zarówno zmian o charakterze eksploatacyjnym / utrzymaniowym, jak i tych będących produktami wytwarzanymi w ramach rozwoju systemów było uporządkowane i zsynchronizowane i nie powodowało utraty spójności środowiska testowego i produkcyjnego. Zamawiający powoła w swojej strukturze ciało, którego celem będzie sterowanie procesem zarządzania zmianą w zakresie zarówno zmian eksploatacyjnych, jak i tych wynikających z rozwoju – Radę ds. Zmian, której przewodniczyć będzie przedstawiciel Zamawiającego – Menedżer ds. Zmian. Ciało to będzie miało charakter decyzyjny w procesie. Odpowiedzialnością wykonawcy będzie skoordynowane i kontrolowane wprowadzanie na środowisko produkcyjne wszystkich typów, ale i wsparcie w roli doradczej Menedżer ds. Zmian, a więc realizacja w szczególności następujących aktywności:
   1) Utrzymywanie dokumentów planów wprowadzenia i wycofania zmian ze środowiska testowego i produkcyjnego.
   2) Analiza i opiniowanie Wniosków o zmianę oraz opracowanie rekomendacji odnośnie ich autoryzacji i obsługi, w tym m.in. weryfikacja wniosku o zmianę w zakresie:
      a. kompletności danych niezbędnych do realizacji przez Wykonawcę,
      b. kompletności danych niezbędnych do aktualizacji bazy konfiguracji,
      c. kompletności danych niezbędnych do aktualizacji katalogów usług,
      d. kompletności danych niezbędnych do aktualizacji systemów monitorowania,
      e. kompletności danych niezbędnych do aktualizacji dokumentacji.
   3) Uczestniczenie w posiedzeniach Rady ds. Zmian.

4) Przygotowanie i opracowanie zmian w systemach w zakresie odpowiedzialności Wykonawcy.
5) Realizacja testowania zmian, w tym projektowanie testów i scenariuszy testowych oraz ich wykonywanie w zakresie odpowiedzialności Wykonawcy.
6) Realizacja (w zakresie odpowiedzialności Wykonawcy) / koordynacja (w zakresie pozostających poza odpowiedzialnością Wykonawcy) wdrożenia zmiany na środowisko testowe i produkcyjne.
7) Obsługa odbioru i zamykania zmian.
8) Aktualizacja dokumentacji utrzymywanej – projektowej, utrzymaniowej i eksploatacyjnej w związku z pojawiającymi się zmianami.

3. Zapewnienie jak najmniejszego negatywnego skutku wprowadzania zmian o charakterze rozwojowym, składających się na całościowe rozwiązanie SIG, na elementy systemów i usługi już na tym środowisku funkcjonujące (zapewnienie ciągłości świadczenia usług) będzie wymagało zaangażowania wykonawcy nie tylko w fazę przekazania, ale również w fazie projektowania (wytwarzania tych zmian) poprzez współpracę z wykonawcami tych zmian zmierzającą do skutecznego wprowadzenia zmian na środowisko produkcyjne. Wykonawca będzie więc również odpowiedzialny za realizację następujących aktywności:

1) Wykonywanie analizy wpływu wdrożenia zmian na środowisko testowe i produkcyjne, ogólne bezpieczeństwo i funkcjonowanie systemów, możliwość utrzymania systemów, w tym identyfikacja elementów w organizacji utrzymania, które powinny ulec dostosowaniu dla wprowadzanej zmiany / systemu.
2) Weryfikacja kompletności przekazywanego rozwiązania (pod względem możliwości jego wdrożenia i późniejszego utrzymania), wsparcie eksperckie w procesie odbioru systemów i zmian.
3) Przygotowywanie / dostosowanie środowiska testowego i produkcyjnego dla planowanych do wdrożenia zmian.
4) Realizacja testów przekazywanych rozwiązań na środowisku testowym przed ich wdrożeniem na produkcję w zakresie wspólnych dla SIG warstw infrastruktury.
5) Realizacja wdrożenia rozwiązań na środowisko testowe i produkcyjne, w tym w szczególności:
    a) wprowadzanie na środowisko produkcyjne, dostosowanie / konfiguracja infrastruktury sprzętowej,
    b) instalacja i konfiguracja w uzgodnionych lokalizacjach oprogramowania składającego się na rozwiązanie,
    c) udostępnienie użytkownikom / zespołom utrzymaniowo-eksploatacyjnym niezbędnej dla ich działania dokumentacji,
    d) aktualizacja bazy konfiguracji,
    e) aktualizacja katalogów usług,
    f) konfiguracja systemów monitorowania,
    g) aktualizacja utrzymywanej dokumentacji – projektowej, utrzymaniowej i eksploatacyjnej.
6) Stabilizacja wprowadzanych zmian systemów, realizacja przeglądów powdrożeniowych.
7) Bieżąca współpraca z podmiotami budującymi lub rozwijającymi systemy / zmiany podlegające późniejszemu wdrożeniu na środowisko produkcyjne.

12.4.4.1 Produkty procesu

W ramach realizacji działań procesu wykonawca jest zobowiązany do bieżącego utrzymania minimum następujących dokumentów:

Tabela 7. Dokumentacja zarządzania zmianami w usługach

Lp.	Nazwa	Opis / Ramowy zakres	Terminy przekazania
1.	Definicja procesu	Dokument opisu procesu obejmujący co najmniej jego cel, politykę, wyzwalacze, diagram z przebiegiem, opis kroków, opis ról i odpowiedzialności (wraz z tabelą RACI), miary, produkty, kluczowe procedury i instrukcje	Inicjalnie wraz z raportem za 1-wszy m-c utrzymania oraz każdorazowo w terminie 14 dni od modyfikacji
2.	Raport z utrzymania	Dokument cyklicznego raportu w zakresie przynależnym dla procesu, zgodnie z rozdziałem 15.2	Comiesięcznie, zgodnie z cyklem raportowania
3.	Plany wprowadzania i wycofywania zmian	Dokument obejmujący harmonogram wprowadzania / wycofywania zmian zgodnie z obowiązującym zakresem	Zgodnie z procesem Zarządzania Zmianą, minimum comiesięcznie, zgodnie z cyklem raportowania
4.	Dokumentacja projektów zmian	Dokumentacja obejmująca co najmniej projekty / specyfikacje rozwiązań dla zmian, wymagania funkcjonalne i niefunkcjonalne adekwatnie do realizowanej zmiany	Zgodnie z harmonogramem realizacji zmian
5.	Opinie / analizy zmian	Dokumentacja obejmująca analizę wpływu wprowadzania zmian na środowisko produkcyjne adekwatnie do zakresu realizowanej zmiany	Zgodnie z harmonogramem realizacji zmian
6.	Raporty / protokoły z działań w zakresie zarządzania zmianami i ich wdrażaniem	Dokumenty obejmują raporty z wykonanych wdrożeń, wycofań, testów – zawierają co najmniej daty realizacji działań, zakres wykonanych działań (dla testów scenariusze i przypadki testowe), wynik / efekt działań, osoby odpowiedzialne, status i rekomendacje zamykające działania, w tym wnioski i rekomendacje działań naprawczych	Zgodnie z harmonogramem realizacji zmian
7.	Dokumentacja SIG	Dokumentacja zgodnie z zakresem przekazywanym przez wykonawców rozwiązania, aktualizowana w wyniku zmian wprowadzanych na środowisko produkcyjne.	Zgodnie z tabelą w rozdziale 14.2

8.	Dziennik administratora	Dokument dziennika administratora w zakresie przynależnym dla procesu (działania instalacyjno-konfiguracyjne w ramach wprowadzania zmian)	Comiesięcznie, zgodnie z cyklem raportowania

Ponadto efektem działania procesu będzie bieżące aktualizowanie informacji w narzędziach ITSM wspierających działanie procesu.

12.4.5 Zarządzanie konfiguracją

Celem procesu jest utrzymywanie bazy konfiguracji zgodnie z metodyką ITIL. Baza konfiguracji powinna uwzględniać co najmniej :

- elementy sprzętowe,
- elementy oprogramowania,
- lokalizacje,
- użytkowników,
- elementy warstw infrastruktury SIG oraz usługi infrastrukturalne i biznesowe,
- licencje,
- warunki wsparcia technicznego,
- powiązania (relacje) pomiędzy wyżej wymienionymi elementami.

W ramach procesu wykonawca będzie w szczególności odpowiedzialny za realizację następujących aktywności:

1) Inwentaryzacja środowiska testowego i produkcyjnego i identyfikacja elementów konfiguracji obecnych na tych środowiskach, utrzymywanie modelu logicznego infrastruktury składającej się na utrzymywane systemy Zamawiającego,
2) Realizacja bieżącej kontroli zapisów o konfiguracji zawartej w bazie konfiguracji, operacyjne zarządzanie bazą konfiguracji, identyfikacja błędów w Bazie Konfiguracji i ich naprawa.

12.4.5.1 Produkty procesu

W ramach realizacji działań procesu wykonawca jest zobowiązany do bieżącego utrzymania minimum następujących dokumentów:

Tabela 8. Dokumentacja zarządzania konfiguracją

Lp.	Nazwa	Opis / Ramowy zakres	Terminy przekazania
1.	Raport z bazy konfiguracji	Dokumentacja w formie ustalonej z Zamawiającym zawierający aktualny model logiczny infrastruktury oraz bazę elementów konfiguracji.	Inicjalnie wraz z raportem za 1-wszy m-c utrzymania oraz każdorazowo w terminie 5 dni roboczych od modyfikacji

2.	Definicja procesu	Dokument opisu procesu obejmujący co najmniej jego cel, politykę, wyzwalacze, diagram z przebiegiem, opis kroków, opis ról i odpowiedzialności (wraz z tabelą RACI), miary, produkty, kluczowe procedury i instrukcje	Inicjalnie wraz z raportem za 1-wszy m-c utrzymania oraz każdorazowo w terminie 14 dni od modyfikacji
3.	Raport z utrzymania	Dokument cyklicznego raportu w zakresie przynależnym dla procesu, zgodnie z rozdziałem 15.2	Comiesięcznie, zgodnie z cyklem raportowania
4.	Model konfiguracji SIG	Dokument obejmujący definicję elementu konfiguracji, klasy elementów konfiguracji podlegających zarządzaniu oraz zakres informacyjny (parametry) gromadzony dla każdej klasy elementu konfiguracji	Inicjalnie wraz z raportem za 1-wszy m-c utrzymania oraz każdorazowo w terminie 14 dni od modyfikacji
5.	Plany zarządzania konfiguracją	Dokumentacja obejmująca planowane działania związane z realizacją zarządzania konfiguracją (w szczególności inwentaryzacje, weryfikacje i audyty bazy konfiguracji)	Zgodnie z procesem Zarządzania Konfiguracją, minimum comiesięcznie, zgodnie z cyklem raportowania
6.	Dziennik administratora	Dokument dziennika administratora w zakresie przynależnym dla procesu (działania konfiguracyjne)	Comiesięcznie, zgodnie z cyklem raportowania

Ponadto efektem działania procesu będzie bieżące aktualizowanie informacji w narzędziach ITSM wspierających działanie procesu.

12.4.6 Operacyjne utrzymanie i eksploatacja infrastruktury

Zapewnienie ciągłości działania systemów wymaga realizacji szeregu operacyjnych czynności administracyjnych na rzecz składowych tych systemów informatycznych (w tym infrastruktury sprzętowo-programowej). W ramach obszaru wykonawca będzie odpowiedzialny w szczególności za realizację następujących aktywności:

1. Weryfikowanie i aktualizacja procedur utrzymaniowych i eksploatacyjnych.
2. Administrowanie, konfiguracja, strojenie i utrzymanie elementów infrastruktury SIG.
3. Operacyjne wykonywanie czynności administracyjnych i operatorskich dla elementów infrastruktury SIG zgodnie z przygotowywaną, otrzymywaną i utrzymywaną dokumentacją
4. Utrzymanie narzędzi do monitorowania elementów infrastruktury SIG.
5. Współpraca z podmiotami świadczącymi usługi gwarancyjne dla elementów infrastruktury systemów w zakresie realizacji usług gwarancyjnych

Szczegółowe zestawienie odpowiedzialności wykonawcy w ramach operacyjnego utrzymania i eksploatacji infrastruktury zawiera poniższa tabela.

Tabela 9. Zestawienie odpowiedzialności wykonawcy w ramach operacyjnego utrzymania i eksploatacji infrastruktury

Obszary kompetencyjne	Nazwa czynności
Obszar aplikacyjny (oprogramowanie standardowe i dedykowane)	Aktualizacja / instalacja oprogramowania standardowego (w szczególności wgrywanie poprawek oprogramowania systemowego i standardowego)
	Monitoring w zakresie incydentów bezpieczeństwa (w szczególności przegląd alarmów bezpieczeństwa i logów systemowych)
	Realizacja testów przełączeniowych (testy przełączeniowe, testy SPoF)
	Zarządzenie aplikacjami narzędziowymi (np. ArcGis, Geomedia) i bazowymi (np. Apache, Tomcat).
	Aktualizacja i testowanie zmian w zakresie aplikacji narzędziowych i bazowych
	Przygotowanie nowych środowisk aplikacyjnych (testowych i produkcyjnych)
	Rekonfiguracja istniejących środowisk aplikacyjnych (produkcyjnych)
	Testy odtworzeniowe (np. odtwarzanie konfiguracji, parametrów działania)
Obszar wirtualizacji	Konfiguracja środowiska wirtualizacyjnego (w szczególności zmiana parametrów ustawień, konfiguracja switch'y wirtualnych, tworzenie nowych maszyn wirtualnych, konfiguracja przydziału pamięci, mocy, maszyn)
	Monitoring działania środowiska wirtualizacyjnego w zakresie wydajności
	Optymalizacja działania środowiska wirtualizacyjnego (w szczególności zmiana parametrów ustawień, konfiguracja switch'y wirtualnych, konfiguracja przydziału pamięci, mocy, maszyn)
	Realizacja testów przełączeniowych (testy przełączeniowe, testy SPoF)
	Testy odtworzeniowe (np. odtwarzanie konfiguracji, parametrów działania)
	Utrzymanie narzędzia antywirusowego.
Obszar systemów operacyjnych	Aktualizacja / instalacja oprogramowania systemowego (w szczególności wgrywanie poprawek oprogramowania systemowego)
	Monitoring w zakresie incydentów bezpieczeństwa (w szczególności przegląd alarmów bezpieczeństwa i logów systemowych)
	Monitoring w zakresie pojemności i wydajności. Optymalizacja pojemności i wydajności
	Realizacja testów przełączeniowych (testy przełączeniowe, testy SPoF)
	Testy odtworzeniowe (np. odtwarzanie konfiguracji, parametrów działania)
Obszar szyny usług	Konfiguracja oprogramowania standardowego szyny usług
	Monitoring w zakresie incydentów bezpieczeństwa (w szczególności przegląd alarmów bezpieczeństwa i logów systemowych)

	Przygotowanie, publikacja oraz utrzymanie konfiguracji usług biznesowych na szynie usług z uwzględnieniem konkretnych potrzeb np. w zakresie monitorowania usług, zapewnienia właściwych protokołów komunikacyjnych, dostarczenia wymaganych mechanizmów bezpieczeństwa, transmisji załączników, walidacji oraz transformacji komunikatów zgodnie z oczekiwaniami Wykonawcy usługi biznesowej.
	Monitoring i optymalizacja silnika szyny usług (parametryzacja, przegląd kolejek itp.)
	Realizacja testów przełączeniowych (testy przełączeniowe, testy SPoF)
	Testy odtworzeniowe (np. odtwarzanie konfiguracji, parametrów działania)
Obszar infrastruktury serwerowej	Konfiguracja urządzeń (wprowadzenie parametrów pracy do urządzeń)
	Monitoring parametrów działania urządzeń, monitoring środowiskowy (w szczególności monitorowanie wydajności, temperatury, stanu sprzętu, pojemności, itp.)
	Monitoring w zakresie incydentów bezpieczeństwa (w szczególności przegląd alarmów bezpieczeństwa i logów systemowych)
	Realizacja testów przełączeniowych (testy przełączeniowe, testy SPoF) To dotyczy każdej warstwy
	Aktualizacja oprogramowania typu firmware (w szczególności wgrywanie poprawek oprogramowana urządzeń, testowanie działania urządzeń po aktualizacji)
	Instalacja urządzeń (urządzenia nowe i urządzenia po wymianie, wymiana wadliwego sprzętu, zabezpieczenie wadliwego sprzętu wg polityki bezpieczeństwa)
	Realizacja testów przełączeniowych (testy przełączeniowe, testy SPoF)
	Testy odtworzeniowe (np. odtwarzanie konfiguracji, parametrów działania)
Obszar bazy danych	Monitoring i optymalizacja silnika bazy danych (w tym wykrywanie „wąskich gardeł”, przydział pamięci operacyjnej i masowej, monitoring pojemności, strojenie)
	Monitoring parametrów działania urządzeń, monitoring środowiskowy (w szczególności monitorowanie wydajności, temperatury, stanu sprzętu, pojemności, itp.)
	Monitoring serwera bazy danych (monitoring wydajności i pojemności instancji baz danych)
	Monitoring w zakresie incydentów bezpieczeństwa (w szczególności przegląd alarmów bezpieczeństwa i logów systemowych)
	Realizacja testów przełączeniowych (testy przełączeniowe, testy SPoF)
	Zarządzanie silnikiem bazy danych (w szczególności rekonfiguracja parametrów silnika, partycjonowanie baz danych, przydzielanie zasobów)
	Zarządzenia instancją bazy danych (w szczególności rekonfiguracja parametrów instancji bazy danych)
	Tworzenie nowych instancji baz danych wg. wymagań Zamawiającego

	Aktualizacja oprogramowania typu firmware i oprogramowania standardowego będącego elementem rozwiązania sprzętowo-programowym (w szczególności wgrywanie poprawek oprogramowania urządzeń, testowanie działania urządzeń po aktualizacji)
	Strojenie baz danych (m.in. partycjowanie tabel, zakładanie indeksów)
	Testy odtworzeniowe (np. odtwarzanie konfiguracji, parametrów działania)
Obszar storage	Instalacja urządzeń (urządzenia nowe i urządzenia po wymianie, wymiana wadliwego sprzętu, zabezpieczenie wadliwego sprzętu wg polityki bezpieczeństwa)
	Konfiguracja urządzeń w ramach warstwy (wprowadzenie parametrów pracy do urządzeń)
	Monitoring parametrów działania urządzeń, monitoring środowiskowy (w szczególności monitorowanie wydajności, temperatury, stanu sprzętu, pojemności, itp.)
	Monitoring wydajności urządzeń warstwy storage (w szczególności identyfikacja „wąskich gardeł", strojenie)
	Realizacja testów przełączeniowych (testy przełączeniowe, testy SPoF)
	Zarządzanie zasobami storage (tworzenie nowych zasobów, rekonfiguracja)
	Optymalizacja sieci SAN (w szczególności rekonfiguracja parametrów urządzeń sieciowych wykorzystywanych w ramach sieci SAN)
	Monitoring w zakresie incydentów bezpieczeństwa (w szczególności przegląd alarmów bezpieczeństwa i logów systemowych)
	Aktualizacja oprogramowania typu firmware (w szczególności wgrywanie poprawek oprogramowana urządzeń, testowanie działania urządzeń po aktualizacji)
	Testy odtworzeniowe (np. odtwarzanie konfiguracji, parametrów działania)
Obszar sieci	Instalacja urządzeń (urządzenia nowe i urządzenia po wymianie, wymiana wadliwego sprzętu, zabezpieczenie wadliwego sprzętu wg polityki bezpieczeństwa)
	Konfiguracja urządzeń w ramach warstwy (wprowadzenie parametrów pracy do urządzeń)
	Konfiguracja urządzeń HSM (w szczególności generowanie kluczy i wgrywanie certyfikatów)
	Implementacja zasad polityki bezpieczeństwa urządzeń sieciowych, konfiguracja urządzeń sieciowych (firewall, switch, VPN, NLB)
	Monitoring parametrów działania urządzeń, monitoring środowiskowy (w szczególności monitorowanie wydajności, temperatury, stanu sprzętu, pojemności, itp.)
	Monitoring w zakresie incydentów bezpieczeństwa (w szczególności przegląd alarmów bezpieczeństwa i logów systemowych)
	Monitoring wydajności sieci i dostępu do Internetu (monitorowanie NLB, obciążenia routerów i switch'y, styku ISP, sesji BGP)

	Optymalizacja sieci operacyjnej LAN (w szczególności przydzielanie adresów IP hostom, partycjonowanie sieci, rekonfiguracja switchy)
	Zarządzanie bazą użytkowników VPN (w szczególności tworzenie, modyfikowanie, usuwanie użytkowników, nadawanie i odbieranie praw dostępu do VPN, implementacja wymagań polityki bezpieczeństwa)
	Monitoring i optymalizacja rozwiązania równoważenia obciążenia sieciowego – NLB (w tym parametryzowanie rozwiązania)
	Aktualizacja oprogramowania typu firmware (w szczególności wgrywanie poprawek oprogramowana urządzeń, testowanie działania urządzeń po aktualizacji)
	Realizacja testów przełączeniowych (testy przełączeniowe, testy SPoF)
	Testy odtworzeniowe (np. odtwarzanie konfiguracji, parametrów działania)
Obszar środowiska backupowego	Konfiguracja i utrzymanie systemu backupu (w szczególności wgrywanie licencji, instalacja i konfiguracja klientów backupowych na stacjach „klientach")
	Rozszerzanie środowiska o nowe zasoby (taśmy, dyski).
	Konfiguracja urządzeń (wprowadzenie parametrów pracy do urządzeń)
	Monitoring parametrów działania urządzeń, monitoring środowiskowy (w szczególności monitorowanie wydajności, temperatury, stanu sprzętu, pojemności, itp.)
	Realizacja testów przełączeniowych (testy przełączeniowe, testy SPoF)
	Utrzymanie środowiska backupowego (w tym wymiana taśm lub dysków).
	Aktualizacja oprogramowania typu firmware (w szczególności wgrywanie poprawek oprogramowana urządzeń, testowanie działania urządzeń po aktualizacji)
	Instalacja urządzeń (urządzenia nowe i urządzenia po wymianie, wymiana wadliwego sprzętu, zabezpieczenie wadliwego sprzętu wg polityki bezpieczeństwa)
	Monitoring parametrów działania urządzeń, monitoring środowiskowy (w szczególności monitorowanie wydajności, temperatury, stanu sprzętu, pojemności, itp.)
	Monitoring w zakresie incydentów bezpieczeństwa (w szczególności przegląd alarmów bezpieczeństwa i logów systemowych)
	Aktualizacja polityk backupu w zakresie zmian zakresu backupowania danych, przyrostu elementów systemu oraz innych zmian tych polityk.
	Testy odtworzeniowe
Obszar środowiska monitoringu i ServiceDesk	Zaimplementowanie zasad i wytycznych dot. monitorowania w narzędziach / aplikacjach monitoringu, w tym konfiguracja środowiska monitoringu
	Zarządzanie środowiskiem aplikacyjnym monitoringu i ServiceDesk (dodawanie nowych procedur, użytkowników, zasilanie baz ServiceDesk, modyfikacje, rekonfiguracje itp.), w tym w zakresie dopasowania do zmian systemie w wyniku rozbudowy o kolejne komponenty

	Monitoring w zakresie incydentów bezpieczeństwa (w szczególności przegląd alarmów bezpieczeństwa i logów systemowych)
	Realizacja testów przełączeniowych (testy przełączeniowe, testy SPoF)
	Testy odtworzeniowe (np. odtwarzanie konfiguracji, parametrów działania)

W przypadkach, gdy Zamawiający ma zawartą umowę ze Stroną Trzecią obejmującą wsparcie techniczne na dostarczane w ramach rozwoju elementy infrastruktury programowo-sprzętowej (rozumianej jako: infrastruktura sprzętowa, oprogramowanie systemowe, standardowe i narzędziowe) odpowiedzialność za realizację całości lub części ww. czynności (o charakterze aktualizacji, testowania, konfiguracji lub instalacji aplikacji, środowisk lub sprzętu) będzie miała odpowiednia Strona Trzecia. W przypadku realizacji czynności przez Stronę Trzecią Wykonawca jest odpowiedzialny za określenie ram dla działań podmiotu realizującego czynność, koordynację jego działań, sprawowanie nadzoru nad realizowaną czynnością oraz wsparcie odbioru realizacji czynności.

12.4.6.1 Produkty procesu

W ramach realizacji działań procesu wykonawca jest zobowiązany do wytworzenia i bieżącego utrzymania minimum następujących dokumentów:

Tabela 10. Dokumentacja operacyjnego utrzymania i eksploatacji infrastruktury

Lp.	Nazwa	Opis / Ramowy zakres	Terminy przekazania
1.	Procedury administrowania i utrzymania	Dokument instrukcji / procedury obejmujący co najmniej wyzwalacze, opis przebiegu (czynności), opis odpowiedzialności, oczekiwany efekt, zgodnie z przedmiotem instrukcji / procedury	Inicjalnie wraz z raportem za 1-wszy m-c utrzymania oraz każdorazowo w terminie 14 dni od wystąpienia modyfikacji
2.	Raport z utrzymania	Dokument cyklicznego raportu w zakresie przynależnym dla obszaru, zgodnie z rozdziałem 15.2	Comiesięcznie, zgodnie z cyklem raportowania
3.	Dziennik administratora	Dokument dziennika administratora obejmujący co najmniej datę, zakres i opis działania, odpowiedzialnego za działanie, opis wyniku / efektu wykonanego działania, status, uwagi / rekomendacje działań następczych oraz odnośnik do dokumentacji szczegółowo opisującej wykonane działania (raport / protokół z realizowanej czynności)	Comiesięcznie, zgodnie z cyklem raportowania
4.	Raport / protokół z realizowanej	Dokumenty obejmują szczegółowy opis wykonywanej czynności z uwzględnieniem założeń, parametrów	Zgodnie z procedurami administrowania,

	czynności administracyjnej	wstępnych, szczegółowych wyników, wniosków i rekomendacji. Dokument stanowi rozszerzenie wpisów w dzienniku administratora a jego poziom szczegółowości jest uwarunkowany czynnością, której dotyczy	w kolejnym miesięcznym cyklu raportowania jako załącznik do Dziennika administratora

Ponadto efektem działania procesu będzie bieżące aktualizowanie informacji w narzędziach ITSM wspierających działanie procesu.

12.4.7 Monitoring infrastruktury SIG, zarządzanie zdarzeniami i monitorowanie aplikacji dedykowanych

Monitorowanie infrastruktury SIG i analiza danych gromadzonych w ramach monitorowania stanowi podstawę podejmowania decyzji odnośnie realizacji szeregu operacyjnych działań związanych z utrzymaniem i eksploatacją infrastruktury informatycznej. Monitoring infrastruktury będzie realizowany w oparciu o:

- poprzez wdrożone, będące w posiadaniu Zamawiającego narzędzia ITSM m.in. : HP Service Manager, HP Business Service Management, Nagios, Centreon i Nagvis, OpenAudit - do czasu wdrożenia nowych narzędzi ITSM,
- poprzez nowe narzędzia ITSM - po ich wdrożeniu;

W ramach obszaru wykonawca będzie odpowiedzialny za realizację następujących aktywności:

1. Konfiguracja / dostosowanie środowiska monitoringu.
2. Projektowanie, utrzymanie i eksploatacja systemów monitorowania infrastruktury, w tym opracowanie propozycji nowych mierników, strojenia i dostosowania i konfiguracji narzędzi monitorowania oraz wprowadzanie zaakceptowanych przez Zamawiającego zmian i konfiguracja narzędzi monitorujących w oparciu o te zmiany.
3. Bieżące monitorowanie utrzymywanej infrastruktury (w tym dokonywanie przeglądów logów systemowych).
4. Projektowanie i utrzymywanie reguł wykrywania i rejestracji zdarzeń wynikających ze zmian statusów elementów konfiguracji środowiska produkcyjnego
5. Projektowanie i utrzymywanie reguł generowania powiadomień dla zdarzeń o charakterze ostrzeżeń (ang. *warning*).
6. Projektowanie i utrzymywanie reguł kierowania zdarzeń do obsługi w ramach innych procesów utrzymania infrastruktury (np. zarządzanie incydentami, zarządzanie problemami, zarządzanie konfiguracją, itd.).
7. Filtrowanie i kategoryzacja zdarzeń.
8. Sterowanie wykonywaniem działań zaprojektowanych do realizacji w wyniku pojawiania się określonych kategorii zdarzeń (np. ręczna realizacja działań, opracowywanie skryptów do automatycznej reakcji na zdarzenia, itd.).
9. Kontrola realizacji zaprojektowanych reguł dla zarządzania zdarzeniami, przegląd i zamykanie zdarzeń.

10. Opracowanie koncepcji monitorowania infrastruktury SIG oraz aplikacji dedykowanych opisanych w rozdziale 7.6 zgodnie z wymaganiami opisanymi w rozdziale 9.13.1 oraz rozdziale 7.16, w terminie 60 dni od dnia podpisania Umowy.
11. Dostosowanie systemu monitorowania zgodnie z Koncepcją Wdrożenia opracowaną przez Wykonawcę.

W ramach realizacji monitoringu aplikacji dedykowanych Wykonawca będzie odpowiedzialny za następujące parametry:

1. Aktywność aplikacji
   Rozumiana jako bieżąca informacja która aplikacja działa a która nie.
2. Dostępność aplikacji
   Rozumiana jako stosunek ilości czasu w którym wybrana aplikacja jest dostępna w wybranym okresie do ilości czasu (total) w wybranym okresie. Zbieranie i przechowywanie statystyk powinno pozwalać na prezentowanie dostępności w ujęciu godzinowym, dziennym, tygodniowym, miesięcznym, rocznym
3. Wydajność aplikacji
   Rozumiana jako czas odpowiedzi wybranej aplikacji, wyrażony w sekundach
4. Przepustowość aplikacji
   Rozumiana jako ilość połączeń z aplikacją w jednostce czasu - na sekundę
5. Lista użytkowników aplikacji bieżąca i historyczna w wybranym okresie czasu (miesięcznym, rocznym)
6. Rozkład użytkowników aplikacji w kontekście dostępności do wybranych funkcjonalności aplikacji. Statystyka bieżąca i historyczna w wybranym okresie czasu (miesięcznym, rocznym)
7. Rozkład użytkowników aplikacji w kontekście przynależności do jednostek administracyjnych
8. Aktywność użytkowników aplikacji
   Rozumiana jako zestawienie użytkowników, aktywnie korzystających (logujących) z usługi w danym okresie. Zbieranie i przechowywanie statystyk powinno pozwalać na prezentowanie wartości parametru w ujęciu dziennym, tygodniowym, miesięcznym, rocznym.
9. Godzinowe obciążenie aplikacji
   Rozumiane jako ilość połączeń z aplikacją w jednostce czasu – godzina.
10. Podstawowe funkcjonalności i ich realizacja przez aplikacje
    Rozumiane jako zestawienie aplikacji i realizowanych przez nie funkcjonalności w kontekście biznesowym
11. Zasoby sprzętowo – systemowe niezbędne do działania aplikacji
    Rozumiane jako zestawienie niezbędnych zasobów sprzętowo-systemowych do działania aplikacji.
12. Niestandardowe zachowania aplikacji
    Rozumiany jako rejestr zdarzeń niestandardowego zachowania się aplikacji. Zbieranie i przechowywanie statystyk powinno pozwalać na prezentowanie wartości parametru w ujęciu dziennym, tygodniowym, miesięcznym, rocznym.

13. Incydenty i problemy zgłaszane do aplikacji
    Realizacja po stronie narzędzi ITSM

12.4.7.1 Produkty procesu

W ramach realizacji działań procesu wykonawca jest zobowiązany do wytworzenia i bieżącego utrzymania minimum następujących dokumentów:

Tabela 11. Dokumentacja monitoringu infrastruktury i zarządzania zdarzeniami

Lp.	Nazwa	Opis / Ramowy zakres	Terminy przekazania
1.	Definicja procesu	Dokument opisu procesu obejmujący co najmniej jego cel, politykę, wyzwalacze, diagram z przebiegiem, opis kroków, opis ról i odpowiedzialności (wraz z tabelą RACI), miary, produkty, kluczowe procedury i instrukcje	Inicjalnie wraz z raportem za 1-wszy m-c utrzymania oraz każdorazowo w terminie 14 dni od modyfikacji
2.	Raport z utrzymania	Dokument cyklicznego raportu w zakresie przynależnym dla procesu, zgodnie z rozdziałem 15.2	Comiesięcznie, zgodnie z cyklem raportowania
3.	Koncepcja monitorowania rozwiązania SIG	Dokument zgodny zakresem z dostarczoną koncepcją monitorowania rozwiązania SIG	Inicjalnie wraz z raportem za 1-wszy m-c utrzymania oraz każdorazowo w terminie 14 dni od zakończenia modyfikacji
4.	Raporty cząstkowe z monitoringu	Raporty cząstkowe z monitoringu w zakresie co najmniej parametrów wskazanych w obowiązującej koncepcji monitorowania rozwiązania SIG	Comiesięcznie, zgodnie z cyklem raportowania

12.4.8 Zarządzania architekturą

Wykonawca – jako utrzymujący środowisko produkcyjne poszczególnych systemów informatycznych jest odpowiedzialny za zachowanie jego spójności architektonicznej. W ramach procesu wykonawca będzie realizował następujące aktywności:

1. Opiniowanie zmian wprowadzanych na środowisko testowe i produkcyjne pod kątem ich wpływu na architekturę systemów oraz ich zgodności ze standardami architektonicznymi SIG. W szczególności w ramach prac na rzecz Rady Architektury (rola ciała opisana w pkt. 20).
2. Tworzenie i utrzymywanie standardów, wytycznych i procedur.
3. Specyfikowanie wymagań pod kątem przyszłego wdrażania i utrzymania systemów.

4. Nadzór nad utrzymaniem i aktualizacją dokumentacji systemów z zastosowaniem obowiązujących notacji, standardów, metodyk i narzędzi wykorzystywanych w ramach całej dokumentacji Systemu.
5. Uczestniczył w pracach Rady Architektury (rola ciała opisana w pkt. 19).

12.4.8.1 Produkty procesu

W ramach realizacji działań procesu wykonawca jest zobowiązany do bieżącego utrzymania minimum następujących dokumentów:

Tabela 12. Dokumentacja zarządzania architekturą

Lp.	Nazwa	Opis / Ramowy zakres	Terminy przekazania
1.	Definicja procesu	Dokument opisu procesu obejmujący co najmniej jego cel, politykę, wyzwalacze, diagram z przebiegiem, opis kroków, opis ról i odpowiedzialności (wraz z tabelą RACI), miary, produkty, kluczowe procedury i instrukcje	Inicjalnie wraz z raportem za 1-wszy m-c utrzymania oraz każdorazowo w terminie 14 dni od modyfikacji
2.	Raport z utrzymania	Dokument cyklicznego raportu w zakresie przynależnym dla procesu, zgodnie z rozdziałem 15.2	Comiesięcznie, zgodnie z cyklem raportowania
3.	Opinie / analizy zmian	Dokumentacja obejmująca analizę wpływu wprowadzania zmian na środowisko produkcyjne adekwatnie do zakresu realizowanej zmiany (w zakresie zgodności ze standardami architektonicznymi)	Zgodnie z harmonogramem realizacji zmian
4.	Standardy i wytyczne	Dokumentacja obejmująca standardy i wytyczne dla wykonawców pod kątem przyszłego wdrażania i utrzymania systemów	Inicjalnie wraz z raportem za 1-wszy m-c utrzymania oraz każdorazowo w terminie 14 dni od modyfikacji

Ponadto efektem działania procesu będzie bieżące aktualizowanie informacji w narzędziach ITSM wspierających działanie procesu.

12.4.9 Zarządzanie dostawcami

Proces zarządzania dostawcami opiera się na kontrolowaniu, utrzymywaniu, nadzorowaniu pracy i relacji z dostawcami oraz na zarządzaniu umowami potrzebnymi do wspierania usług IT. Proces ma za zadanie rozpoznać wartość wkładu biznesowego danego dostawcy, następnie zbudowanie i zarządzanie relacją z dostawcą, tak aby ten wkład był podtrzymany. Relacje z poszczególnymi dostawcami mają charakter indywidualny i są zarządzane bezpośrednio w procesie zarządzania dostawcami.

Wykonawca w procesie zarządzania dostawcami będzie pełnił istotną rolę. Infrastruktura SIG składa się z elementów, które zostały dostarczone przez różne podmioty. Różnorodne podmioty świadczą usługi na rzecz CODGiK i Zamawiającego, także w zakresie wsparcia technicznego dla dostarczonego sprzętu oraz umów na wsparcie techniczne. W szczególności Wykonawca będzie zobowiązany do koordynacji własnych poddostawców.

Wykonawca będzie zarządzał dostawcami zgodnie z ITIL 2011 tak aby m.in:

- zapewnić, że kontrakty z dostawcami zewnętrznymi oraz wszelkie uzgodnienia z dostawcami są powiązane z potrzebami organizacji,
- wspierać dla wszystkich uzgodnionych celów organizacje w zakresie dostaw,
- zarządzanie relacjami z dostawcami i ich wydajnością,
- negocjowanie oraz akceptowanie umów z dostawcami oraz zarządzanie tymi relacjami przez cały cykl ich aktywności,
- utrzymanie odpowiedniej polityki dostawczej,
- wsparcie dla dostawców oraz procesów SCMIS,

W tym celu Wykonawca:

1. wdroży system zarządzania dostawcami i umowami (ang. SCMIS),
2. będzie sporządzał raporty wydajności dostawców i umów,
3. organizował spotkania przeglądowe dostawców i umów,
4. przygotuje plan doskonalenia usługi dostawców.

Szczegółowy zakres prac w obszarze Wykonawca ustali z Zamawiającym po podpisaniu umowy.

12.4.10 Zarządzanie wydaniami i wdrożeniami

Zakres działania procesu zarządzania wydaniami i wdrożeniami obejmuje procesy, systemy i funkcje potrzebne do zbudowania, przetestowania i rozmieszczenia wydań, w celu ich zaktywizowania. Ponadto koncentruje się na ustalaniu specyfiki usług w pakietach projektu usługi oraz, formalnie, przekazuje używanie usługi na etap eksploatacji usług.

Wykonawca będzie uczestniczył w procesie zarządzania wydaniami i wdrożeniami zgodnie z ITIL 2011 tak aby m.in.:

- Zdefiniować i stworzyć plany zarządzania wydaniami i wdrożeniami,
- stworzyć i testować pakiety wydań,
- rozlokowywać pakiety wydań zgodnie z wcześniej powstałym planem,

- zapewniać warunki tak aby Zamawiający i jego Interesariusze wiedzieli, że zmiany są odpowiednio zarządzane
- zapewniać warunki tak, że nowe albo zmienione usługi mogą być dostarczane w zgodzie z ustalonymi wcześniej poziomami wykorzystania i gwarancją,
- zapewniać warunki tak, że klienci, użytkownicy i pracownicy IT będą mieli dostęp do odpowiedniej wiedzy

W tym celu Wykonawca:

- Będzie utrzymywał i przekazywał rejestr nowych, zmienionych lub odrzuconych usług,
- Będzie utrzymywał i przekazywał rejestr nowej lub zmienionej dokumentacji,
- Wytworzy propozycję umów SLA oraz umów OLA,
- Będzie utrzymywał i przekazywał rejestr nowych lub zmieniony usług,
- aktualizował plany zarządzania ITSCM oraz potencjałem wykonawczym.

Szczegółowy zakres prac w obszarze Wykonawca ustali z Zamawiającym po podpisaniu umowy.

12.4.11 Koordynacja projektowania

Koordynacja projektowanie jest procesem mającym zapewnić, że zamiary i cele na danym etapie projektowania zostały spełnione. Proces zapewnia odpowiedni punkt koordynacji i kontroli w odniesieniu do wszystkich działań i procesów na danym etapie cyklu życia usługi.

Wykonawca będzie uczestniczył w procesie koordynacji projektowania zgodnie z ITIL 2011 tak aby m.in.:

- zapewniać zgodnego z celami Zamawiającego projektu odpowiednich usług, zarządzania systemami informatycznymi, architektury, technologii, procesów, metryk, w celu zaspokojenia bieżących i zmieniających się potrzeb i wymogów biznesowych,
- planować i koordynować wszystkie zaprojektowane działania,
- tworzyć pakiet projektu usługi w oparciu o kartę usługi oraz zgłoszenie zmiany,
- zapewniać warunki tak, że odpowiednie projekty usług zostaną stworzone oraz, że zostaną przekazane do fazy przekazania usługi, jako zaakceptowane,
- zarządzać powiązaniami z fazami strategii usług oraz przekazania usług,
- rozwijać wydajność i efektywność projektu, działań i procesów związanych z daną usługą

W tym celu Wykonawca:

- Będzie utrzymywał kompleksowy i spójny zestaw projektów usług i SDP,

- Będzie współtworzył architekturę rozwiązania
- Będzie tworzył/zaktualizuje systemy zarządzania, procesy, metryki i metody metryczne

Szczegółowy zakres prac w obszarze Wykonawca ustali z Zamawiającym po podpisaniu umowy.

12.4.12 Zarządzanie wiedzą

Zarządzanie wiedzą jest trwającym przez cały cykl życia usługi procesem, którego znaczenie jest ogromne na wszystkich etapach zarządzania usługami.

Wykonawca będzie uczestniczył w procesie zarządzania wiedzą zgodnie z ITIL 2011 tak aby m.in.:

- rozwijać procedury zarządzania podejmowanymi decyzjami, poprzez zapewnienie, że pomocne i bezpieczne dane, informacje i wiedza są dostępne,
- umożliwiać dostawcą usług w byciu bardziej wydajnym i rozwoju jakości usługi, wzrostu satysfakcji oraz redukcji kosztów usługi,
- utrzymywać system zarządzania wiedzą o usługach, zapewniający kontrolowany dostęp do odpowiednich zasobów wiedzy, informacji oraz danych;
- zbierać, analizować, dzielić się oraz utrzymywać zasoby wiedzy, informacji i danych w całej organizacji

W tym celu Wykonawca:

- zidentyfikuje i zgromadzi wszelkie zasoby wiedzy potrzebne do świadczenia przez niego przedmiotu zamówienia (w szczególności dokumentację opisaną w punkcie 11.6)
- zaktualizuje/uruchomi i zasili system zarządzania wiedzą zebranymi zasobami wiedzy.
- będzie cyklicznie dokonywał przeglądu potrzebnej wiedzy, czynnie ją pozyskiwał i zasilał system zarządzania wiedzą.

Szczegółowy zakres prac w obszarze Wykonawca ustali z Zamawiającym po podpisaniu umowy.

12.4.13 Zarządzanie zasobami i konfiguracją usług

Zasoby usług, które muszą być zarządzane, aby dostarczyć daną usługę są w ITIL znane jako elementy konfiguracji. Zakres działań procesu obejmuje zarządzanie cyklem życia każdego właściwie elementu konfiguracji. Proces ten zajmuje się także powiązaniami z zewnętrznymi i wewnętrznymi dostawcami usług, którzy korzystają z zasobów i elementów konfiguracji, które wymagają ścisłej kontroli z racji, tego że są aktywami wspólnymi.

Proces zarządzania środkami trwałymi utrzymuje z kolei rejestr zasobów, w którym są zapisane informacje finansowe dotyczące wszystkich środków trwałych organizacji. Proces ten zazwyczaj nie

podlega tym samym kontrolnym procedurom co usługi IT, ale z kolei proces zarządzania zasobami i konfiguracją usług musi zapewnić odpowiednia opiekę środkom trwałym, wykorzystywanym przez procesy IT.

Wykonawca będzie uczestniczył w procesie zarządzania zasobami i konfiguracją usług zgodnie z ITIL 2011 tak aby m.in.:

- Zapewniać warunki tak, że zasoby zostaną zidentyfikowane, kontrolowane, zarządzane i chronione podczas całego cyklu trwania procesu,
- identyfikować, kontrolować, zapisywać, raportować i weryfikować usługi oraz elementy konfiguracji, z uwzględnieniem ich atrybutów i relacji,
- zapewniać integralności elementów konfiguracji z poszczególnymi konfiguracjami poprzez utrzymania odpowiedniej informacji konfiguracyjnej na jej historycznym, zaplanowanym lub obecnym poziomie, w systemie zarządzania konfiguracją,
- wspieranie wydajnościowego i efektywnego procesu zarządzania usługami poprzez zapewnienie odpowiednich informacji o konfiguracji

W tym celu Wykonawca będzie:

- wprowadzał do systemu zarządzania konfiguracją nowe lub zmienione zapisy konfiguracji
- aktualizował dane o atrybutach i relacjach między elementami konfiguracji,
- wykonywał raporty statusu, audyty

Szczegółowy zakres prac w obszarze Wykonawca ustali z Zamawiającym po podpisaniu umowy.

12.4.14 Planowanie i wsparcie przekazania

Planowanie i wsparcie przekazania koncentruje się głównie na utrzymaniu odpowiedniej polityki, standardów oraz modeli przekazywania usług, przeprowadzenie większych zmian w toku całego procesu usług , ustalanie priorytetów i koordynowanie dostaw zasobów potrzebnych do wykonania wielu przekazań w tym samym czasie, rozplanowanie budżetu i zasobów procesu przekazania usług, przegląd i rozwój wydajności procesu planowania i wsparcia przekazania

Wykonawca będzie uczestniczył w procesie planowania i wsparcia przekazania zgodnie z ITIL 2011 tak aby m.in.:

- planować i koordynować przekazanie zasobów usług w ramach struktur IT oraz do wszystkich projektów, dostawców i grup pracowniczych - gdzie jest to potrzebne,

- ustalać nowe lub zmieniać obecne usługi zgodnie z przewidywanymi cenami, jakością oraz czasem,
- ustalać nowe lub zmodyfikować obecne systemy i narzędzia informowania Zamawiającego, technologii, struktur zarządzania, procesów zarządzania usługami czy miar i metod pomiaru, w celu realizacji potrzeb organizacji biznesowej,
- zapewniać plany, które umożliwią Zamawiającemu zmianę projektów, w celu powiązania ich z etapem przekazania projektów,
- identyfikować, kontrolować i zarządzać zagrożeniami,
- monitorować i rozwijać wydajności usług w toku trwania całego cyklu przekazania usług;

W tym celu Wykonawca będzie:

- współtworzył strategia przekazania i budżet
- współtworzył zintegrowany zestaw planów przekazania usług

Szczegółowy zakres prac w obszarze Wykonawca ustali z Zamawiającym po podpisaniu umowy.

12.4.15 Zarządzanie bezpieczeństwem informacji i uprawnieniami dostępu

Wykonawca będzie świadczył Usługę Zarządzania bezpieczeństwem Systemu zgodnie z obowiązującymi unormowaniami prawnymi i standardami bezpieczeństwa teleinformatycznego oraz regulacjami wewnętrznymi, współpracując z osobami odpowiedzialnymi za obszar bezpieczeństwa Zamawiającego. W ramach procesu wykonawca będzie odpowiedzialny za realizację następujących aktywności:

1. Zapewnienie przestrzegania przez Wykonawcę uzgodnionych przez Wykonawcę z Zamawiającym procedur bezpieczeństwa.
2. Wykonywanie analizy ryzyka dla elementów systemów objętych utrzymaniem, w tym:
    1) identyfikowanie zagrożeń i podatności zasobów,
    2) analiza ryzyk związanych ze zidentyfikowanymi zagrożeniami i podatnościami oraz monitorowanie ryzyk szczątkowych,
3. Monitorowanie poziomu bezpieczeństwa systemów m.in. poprzez:
    1) monitorowanie poufności, integralności i dostępności danych i informacji gromadzonych w systemach, zgodnie z obowiązującymi regulacjami prawnymi i wewnętrznymi Zamawiającego
    2) monitorowanie dostępności usług i komponentów Systemu,
    3) monitorowanie i obsługa incydentów bezpieczeństwa Systemu (m.in. poprzez przegląd logów systemowych),
    4) monitorowanie dostawców i innych współpracujących organizacji poprzez kontrolę uprawnień oraz kontrolę formalną oprogramowania i sprzętu wykorzystywanego do przetwarzania informacji Systemu,

5) monitorowanie infrastruktury systemu pod względem pochodzenia oprogramowania wykorzystywanego w systemach,
6) monitorowanie oprogramowania pod kątem wspierania używanej wersji przez producenta oraz zapewnienia obsługi gwarancyjnej i serwisowej przez producenta

4. Śledzenie aktualizacji komponentów systemów związanych z bezpieczeństwem i rekomendowanie ich wdrożenia zgodnie z procesem zarządzania Zmianami.
5. Weryfikacja wpływu wprowadzonych na środowisku testowym i produkcyjnym zmian na bezpieczeństwo systemu.
6. Operacyjne zarządzanie uprawnieniami dostępu użytkowników do usług i elementów infrastruktury systemów.
7. Realizacja zarządzania Incydentami bezpieczeństwa w ramach procesu zarządzania incydentami.
8. Projektowanie i utrzymywanie dokumentacji bezpieczeństwa, w tym polityki bezpieczeństwa w zakresie utrzymywanych elementów systemów.
9. Realizacja kwartalnych audytów i kontroli poziomu bezpieczeństwa systemów.

12.4.15.1 Produkty procesu

W ramach realizacji działań procesu wykonawca jest zobowiązany do bieżącego utrzymania minimum następujących dokumentów:

Tabela 13. Dokumentacja zarządzania bezpieczeństwem informacji i uprawnieniami dostępu

Lp.	Nazwa	Opis / Ramowy zakres	Terminy przekazania
1.	Definicja procesu	Dokument opisu procesu obejmujący co najmniej jego cel, politykę, wyzwalacze, diagram z przebiegiem, opis kroków, opis ról i odpowiedzialności (wraz z tabelą RACI), miary, produkty, kluczowe procedury i instrukcje	Inicjalnie wraz z raportem za 1-wszy m-c utrzymania oraz każdorazowo w terminie 14 dni od modyfikacji
2.	Raport z utrzymania	Dokument cyklicznego raportu w zakresie przynależnym dla procesu, zgodnie z rozdziałem 15.2	Comiesięcznie, zgodnie z cyklem raportowania
3.	Polityka bezpieczeństwa	Dokument obejmuje pryncypia zarządzania bezpieczeństwem w zakresie rozwiązania SIG	Inicjalnie wraz z raportem za 1-wszy m-c utrzymania oraz każdorazowo w terminie 14 dni od modyfikacji
4.	Procedury i instrukcje bezpieczeństwa	Dokument instrukcji / procedury obejmujący co najmniej wyzwalacze, opis przebiegu (czynności), opis odpowiedzialności, oczekiwany efekt, zgodnie z przedmiotem instrukcji / procedury	Zgodnie z procesem Zarządzania Bezpieczeństwem, w kolejnym miesięcznym cyklu raportowania po wykonaniu testów /

			przeglądów
5.	Dokument analizy ryzyka dla infrastruktury IT	Dokument obejmujący co najmniej zestawienie i klasyfikację elementów infrastruktury składającej się na rozwiązanie SIG, zestawienie podatności dla tych elementów, zestawienie rozważanych scenariuszy wykorzystania tych podatności, opis środków zaradczych, zastosowanych zabezpieczeń oraz rekomendowanych działań.	Comiesięcznie, zgodnie z cyklem raportowania
6.	Dziennik administratora	Dokument dziennika administratora w zakresie przynależnym dla procesu (w szczególności działania weryfikacyjne, przeglądowe, audytowi, związane z obsługą stanów zagrożenia bezpieczeństwa)	Comiesięcznie, zgodnie z cyklem raportowania

Ponadto efektem działania procesu będzie bieżące aktualizowanie informacji w narzędziach ITSM wspierających działanie procesu.

12.4.16 Utrzymanie narzędzi ITSM

Wykonawca będzie realizował powierzone mu zadania z wykorzystaniem będących własnością zamawiającego narzędzi ITSM, przy czym:

- poprzez wdrożone, będące w posiadaniu Zamawiającego narzędzia ITSM m.in. : HP Service Manager, HP Business Service Management, Nagios, Centreon i Nagvis, OpenAudit - do czasu wdrożenia nowych narzędzi ITSM,
- poprzez nowe narzędzia ITSM - po ich wdrożeniu;

Wykonawca będzie odpowiedzialny za realizację wszystkich działań związanych z utrzymaniem, administrowaniem, konfigurowaniem, eksploatacją, w tym zasilaniem danymi i informacjami wytwarzanymi w ramach realizacji przedmiotu zamówienia.

Wszystkie umieszczone w narzędziach ITSM i wytwarzane informacje i dane, a także widoki, konfiguracja są własnością Zamawiającego.

W przypadku, gdy realizacja ww. działań związanych z utrzymaniem, administrowaniem, konfigurowaniem, eksploatacją, w tym zasilaniem danymi i informacjami będzie wymagała zestawienia przez Wykonawcę dodatkowych środowisk programowo-sprzętowych (np. o charakterze testowym lub przedprodukcyjnym) Wykonawca zobowiązany jest do ich przygotowania we własnym zakresie w ramach zasobów własnych.

12.4.16.1 Wykorzystanie narzędzi wspierających

Wszelkie działania wykonawcy w obszarze utrzymania i serwisu (rozdziały i 12.4) będą realizowane z wykorzystaniem narzędzi ITSM będących w posiadaniu Zamawiającego, przy czym:

- poprzez wdrożone, będące w posiadaniu Zamawiającego narzędzia ITSM m.in. : HP Service Manager, HP Business Service Management, Nagios, Centreon i Nagvis, OpenAudit - do czasu wdrożenia nowych narzędzi ITSM,
- poprzez nowe narzędzia ITSM - po ich wdrożeniu;

Wszelkie odstępstwa od wykorzystania narzędzi Zamawiającego każdorazowo wymagają zgody Zamawiającego, a wykorzystanie innych narzędzi bez zgody jest traktowane jako realizacja działań bez wsparcia narzędziowego. W przypadku decyzji o wykorzystaniu innych narzędzi niż będące w posiadaniu Zamawiającego Wykonawca jest zobowiązany do zapewnienia bieżącego, nielimitowanego dostępu do tych narzędzi na prawach administratora i czytelnika. Ponadto Wykonawca przekaże zamawiającemu dokumentację administrowania i użytkowania tych dodatkowych narzędzi.

Dane gromadzone w narzędziach (zarówno będących w własnością zamawiającego, jak i dodatkowych narzędziach wykonawcy) stanowią własność Zamawiającego. Wykonawca jest zobowiązany do bieżącego wykonywania kopii zapasowych ww. danych zgodnie z miesięcznym cyklem raportowania, a wraz z zamknięciem umowy do przekazania Zamawiającemu archiwalnej oraz aktualnej postaci danych, zgodnie z określonym przez Zamawiającego formatem.

12.4.16.2 Produkty procesu

W ramach realizacji działań procesu Wykonawca jest zobowiązany do bieżącego utrzymania minimum następujących dokumentów:

Tabela 14. Dokumentacja utrzymania narzędzi ITSM

Lp.	Nazwa	Opis / Ramowy zakres	Terminy przekazania
1.	Dokumentacja konfiguracji narzędzi ITSM	Dokument opisu procesu obejmujący co najmniej założenia poczynione przy dostosowywaniu, konfiguracji narzędzi, udokumentowanie projektowanych widoków, udokumentowanie zmian w zastosowanych strukturach danych, dostępie do narzędzia. Dla narzędzi dostarczanych przez wykonawcę o których mowa w podrozdziale „Wykorzystanie narzędzi wspierających” dokumentacja	Inicjalnie wraz z raportem za 1-wszy m-c utrzymania oraz każdorazowo w terminie 14 dni od modyfikacji

		obejmie ponadto podręcznik użytkownika i administratora narzędzi.	
2.	Raport z utrzymania	Dokument cyklicznego raportu w zakresie przynależnym dla obszaru, zgodnie z rozdziałem 15.1	Comiesięcznie, zgodnie z cyklem raportowania
3.	Dziennik administratora	Dokument dziennika administratora w zakresie przynależnym dla obszaru (w szczególności działania związane z utrzymaniem, administrowaniem, konfigurowaniem, eksploatacją, zasilaniem danymi i informacjami).	Comiesięcznie, zgodnie z cyklem raportowania

Ponadto efektem działania procesu będzie bieżące aktualizowanie informacji w narzędziach ITSM wspierających działanie procesu.

12.5 Utrzymanie dokumentacji procesów utrzymania i serwisu

Wykonawca będzie aktualizował dokumenty z definicją wszystkich procesów wymienianych w rozdziałach 14.1 i 14.2. w przypadku zmian realizacji procesu w terminie nieprzekraczającym 14 dni od wystąpienia tych zmian. Ponadto wykonawca w ww. terminie dokona weryfikacji istniejących procedur utrzymaniowych w zakresie zgodności z przyjętą formułą utrzymaniową oraz przekaże rekomendacje zmian do wprowadzenia w procedurach.

13 Wykorzystywane narzędzia do monitorowania systemów oraz zarządzania usługami i utrzymaniem systemów

13.1 Monitorowanie systemu

1. Centralny system monitoringu dla infrastruktury SIG jest oparty na aktualnie będącym w posiadaniu Zamawiającego oprogramowaniu, m.in. na:
    - HP BSM,
    - Nagios, Nagvis, Centreon,
    - OpenAudit,
    - Cacti, Kibana, Elastic Search, awstats,
    - Mechanizmy środowiska Oracle Exadata oraz Oracle Database,
    - Mechanizmów stanowiących elementy systemów informatycznych (dziedzinowych),
    - Narzędzi wbudowanych w oprogramowanie standardowe oraz rozwiązania sprzętowe,
    - Dedykowane mechanizmy np. skrypty.

Wykonawca jest odpowiedzialny za realizację czynności związanych z monitorowaniem infrastruktury rozwiązania. Wykonawca do czasu wdrożenia nowych narzędzi ITSM będzie realizował powierzone mu zadania związane z monitorowaniem SIG z wykorzystaniem narzędzi, o których mowa w pkt. 1 oraz poprzez nowe narzędzia ITSM, po ich wdrożeniu.

14 Parametry obowiązujące Wykonawcę

W poniższych rozdziałach wskazane zostały parametry które zobowiązany jest zapewnić wykonawca w zakresie realizowanych przez siebie zadań.

14.1 Parametry infrastruktury w poszczególnych warstwach

14.1.1 Wartości parametrów

1. Wykonawca zapewni następujące wartości parametrów dotyczących poszczególnych warstw infrastruktury. Poniższe parametry mają być zachowane w okresach nie obejmujących:

1) uzgodnionych z Zamawiającym okien serwisowych

2) realizacji usług serwisowych przez Zamawiającego bądź innych wykonawców świadczących usługi gwarancyjne na dostarczone elementy infrastruktury

2. Wykonawca zapewni uwzględnienie ww. wyłączeń w automatycznych raportach SLA z monitoringu usług.

Tabela 15. Parametry SLA dla obszaru monitorowania

Lp.	Parametr	Oczekiwana wartość środowisk testowych			Oczekiwana wartość środowisk produkcyjnych		
		dzienna	tygodniowa	miesięczna	dzienna	tygodniowa	miesięczna
1.	Dostępność pojedynczego serwera fizycznego	95%	99%	99%	95%	99%	99%
2.	Dostępność przestrzeni dyskowych (macierze)	95%	99%	99%	95 %	99%	99%
3.	Dostępność poszczególnej instancji baz danych	95%	99%	99%	95%	99%	99%
4.	Dostępność	95%	99%	99%	95%	99%	99%

	urządzeń sieciowych						
5.	Dostępność szyny usług	95%	99%	99%	95%	99%	99%
6.	Dostępność systemów backupowych	95%	99%	99%	95%	99%	99%
7.	Dostępność narzędzi wirtualizacyjnych	95%	99%	99%	95%	99%	99%
8.	Dostępność serwerów wirtualnych	80%	90%	95%	95%	99%	99%
9.	Dostępność narzędzi Service Desk i monitoringu	95%	99%	99%	95%	99%	99%
10.	Dostępność aplikacji i narzędzi standardowych	80%	90%	95%	95%	99%	99%
11.	Dostępność usługi zewnętrznych sieci	95%	99%	99%	95%	99%	99%
12.	Dostępność usługi VPN	95%	99%	99%	95%	99%	99%
13.	Dostępność usług	80%	90%	95%	95%	99%	99,5%

	biznesowych						
14.	Obciążenie zasobów (CPU, RAM, przestrzeń dyskowa) dla serwerów fizycznych i maszyn wirtualnych	<=95%			<=90%		

Wykonawca ponosi wyłączną odpowiedzialność za niedostępność powyższych elementów infrastruktury. W przypadku fizycznej awarii elementu infrastruktury Wykonawca ponosi odpowiedzialność za czas niedostępności elementu infrastruktury liczony do momentu zgłoszenia awarii do strony trzeciej (gwaranta) lub przekazania informacji do Zamawiającego w przypadku braku gwaranta.

Wskazane w powyższej tabeli parametry obowiązują **jednostkowo** – dla pojedynczych elementów infrastruktury programowo-sprzętowej (np. dla każdego serwera, aplikacji, itd.) w jednostce czasu określonej w powyższej tabeli.

Wykonawca będzie raportował parametry z uwzględnieniem powyższych założeń i będzie z nich rozliczany. Wykonawca zapewni możliwość automatycznego generowania wymienionych parametrów oraz dostępność *on-line* w narzędziach ITSM na potrzebę weryfikacji przez Zamawiającego.

14.2 Parametry dla realizowanych zadań i aktywności Wykonawcy

14.2.1 Wartości parametrów

Wykonawca będzie świadczył usługi z zakresu przedmiotu zamówienia zgodnie z następującymi parametrami jakościowymi:

Tabela 16. Parametry SLA dla obszaru serwisu i utrzymania

Lp.	Parametr	Oczekiwana wartość		
PARAMETRY OBSZARU SERWISU				
		krytycznym	**pilnym**	**standardowym**
1.	Czas reakcji na zgłoszenie	15 min.	30 min.	1 h

2.	Czas obsługi incydentu (dla incydentów przynależnych Wykonawcy)	2 h	8 h	16 h
3.	Czas udokumentowania opracowanego rozwiązania incydentu i umieszczenia w bazie wiedzy	2 dni robocze		
4.	Czas opracowania standardowego modelu dla incydentu	5 dni roboczych		
5.	Czas wyeskalowania incydentu (dla incydentów nie przynależnych Wykonawcy)	30 min.		
6.	Częstotliwość przeglądu i analizy krytycznych i pilnych incydentów	co najmniej 1 raz w miesiącu		
7.	Czas zarejestrowania rekordu problemu od momentu zgłoszenia	4 h		
8.	Czas opracowania i wdrożenia rozwiązania docelowego dla problemu	10 dni roboczych lub w czasie uzgodnionym z Zamawiającym		
9.	Czas udokumentowania opracowanego rozwiązania problemu i umieszczenia w bazie wiedzy	2 dni robocze		
PARAMETRY OBSZARU UTRZYMANIA INFRASTRUKTURY				
12.	aktualność katalogu usług	95%		
13.	czas aktualizacji informacji o usłudze w katalogu usług	5 dni roboczych		
14.	częstotliwość aktualizacji bazy licencji i warunków wsparcia technicznego	co najmniej 1 raz w miesiącu		

<table>
<tr><td>15.</td><td>częstotliwość wykonywania analizy trendów utylizacji zasobów poszczególnych elementów infrastruktury</td><td colspan="3">co najmniej 1 raz w miesiącu</td></tr>
<tr><td rowspan="2">16.</td><td rowspan="2">czas zaopiniowania zmiany: w tym oceny RFC (wniosku o zmianę)</td><td>pilnych</td><td>normalnych</td><td>standardowych</td></tr>
<tr><td>1h</td><td>Do 3 dni roboczych</td><td>Do 4h roboczych</td></tr>
<tr><td rowspan="2">17.</td><td rowspan="2">czas obsługi zmiany dla zmian</td><td>pilnych</td><td>normalnych</td><td>standardowych</td></tr>
<tr><td>3h</td><td>na podstawie terminu ustalonego w RFC (pkt. 14)</td><td>4h lub w czasie uzgodnionym z Zamawiającym</td></tr>
<tr><td>18.</td><td>czas na aktualizację dokumentacji po wprowadzeniu zmiany (dla dokumentacji aktualizowanej przez Wykonawcę)</td><td colspan="3">30 dni roboczych</td></tr>
<tr><td>19.</td><td>czas aktualizacji informacji o elemencie konfiguracji w bazie konfiguracji</td><td colspan="3">5 dni roboczych</td></tr>
<tr><td>20.</td><td>poziom aktualności bazy konfiguracji (poziom rozbieżności wykazanych w bazie podczas przeglądu / kontroli konfiguracji względem faktycznego stanu środowiska produkcyjnego)</td><td colspan="3">co najwyżej 3% elementów konfiguracji</td></tr>
<tr><td>21.</td><td>częstotliwość przeglądów planów awaryjnych / planów zapewnienia ciągłości</td><td colspan="3">co najmniej 1 raz na kwartał</td></tr>
<tr><td>22.</td><td>częstotliwość testowania planów awaryjnych / planów zapewnienia ciągłości</td><td colspan="3">co najmniej 1 raz na półrocze</td></tr>
<tr><td>23.</td><td>procent czynności administracyjnych pokrytych</td><td colspan="3">95%</td></tr>
</table>

	dokumentacją	
24.	procent parametrów wymaganych objętych monitorowaniem	95%

Wskazane w powyższej tabeli parametry z pozycji 1-5, 7-11, 16-19 obowiązują wykonawcę dla każdego realizowanego działania, incydentu, zmiany, elementu konfiguracji, itd.

Wskazane w powyższej tabeli parametry z pozycji 14-15, 21 stanowią pojedyncze wartości raportowane i obowiązujące wykonawcę.

Wykonawca będzie raportował parametry z uwzględnieniem powyższych założeń i zgodnie z nimi będzie rozliczany. Wykonawca zapewni możliwość automatycznego generowania wymienionych parametrów oraz dostępność *on-line* w narzędziach:

- poprzez wdrożone, będące w posiadaniu Zamawiającego narzędzia ITSM m.in. : HP Service Manager, HP Business Service Management, Nagios, Centreon i Nagvis, OpenAudit - do czasu wdrożenia nowych narzędzi ITSM,
- poprzez nowe narzędzia ITSM - po ich wdrożeniu;

na potrzebę weryfikacji przez Zamawiającego.

14.2.2 Metoda wyliczania parametrów

Tabela 17. Sposób wyliczenia parametrów SLA dla obszaru serwisu i utrzymania

Lp.	Parametr	Metoda wyliczania
PARAMETRY OBSZARU SERWISU		
1.	Czas reakcji na incydent	zgodnie z definicją w słowniku
2.	Czas obsługi incydentu (dla incydentów przynależnych wykonawcy)	zgodnie z definicją w słowniku
3.	Czas udokumentowania opracowanego rozwiązania i umieszczenia w bazie wiedzy	czas od momentu zamknięcia incydentu, do momentu umieszczenia rozwiązania w bazie wiedzy
4.	Czas opracowania standardowego modelu dla incydentu	**czas od momentu zamknięcia incydentu, który inicjuje potrzebę opracowania modelu do momentu** umieszczenia instrukcji / procedury w narzędziu ITSM
5.	Czas wyeskalowania incydentu (dla incydentów nie przynależnych wykonawcy)	**czas od momentu zgłoszenia incydentu do jego przekazania do obsługi po stronie zewnętrznego** wykonawcy

6.	częstotliwość przeglądu i analizy krytycznych i pilnych incydentów	czas który upłynął od poprzedniej realizacji działania
7.	Czas zarejestrowania rekordu problemu od momentu zgłoszenia	czas od momentu zgłoszenia problemu do jego zarejestrowania w narzędziu ITSM
8.	Czas opracowania i wdrożenia rozwiązania docelowego dla problemu	czas od momentu zgłoszenia problemu do wdrożenia rozwiązania docelowego
9.	Czas udokumentowania opracowanego rozwiązania i umieszczenia w bazie wiedzy	opracowania rozwiązania do jego umieszczenia w bazie wiedzy
PARAMETRY OBSZARU UTRZYMANIA INFRASTRUKTURY		
13.	czas aktualizacji informacji o usłudze w katalogu usług	wartość procentowa stosunku liczby usług w katalogu usług nieaktualnych (nieaktualna dowolna informacja / parametr przechowywany o usłudze / brak usługi w narzędziu ITSM) do ogólnej wymaganej liczby usług w katalogu usług
14.	częstotliwość aktualizacji bazy licencji i warunków wsparcia technicznego,	**czas który upłynął od poprzedniej realizacji działania**
15.	częstotliwość wykonywania analizy trendów utylizacji zasobów poszczególnych elementów infrastruktury	czas który upłynął od poprzedniej realizacji działania
16.	czas zaopiniowania zmiany: w tym oceny RFC (wniosku o zmianę)	czas od zgłoszenia zmiany do momentu przekazania opinii Zamawiającemu
17.	czas obsługi zmiany	czas od zaakceptowania wniosku o zmianę do terminu ustalonego zgodnie z tabelą w pkt. 11.2.1
18.	czas na aktualizację dokumentacji po wprowadzeniu zmiany (dla dokumentacji aktualizowanej przez Wykonawcę)	liczba dni roboczych, która upłynęła od wprowadzenia zmiany do przekazania Zamawiającemu zaktualizowanej dokumentacji, do ww. czasu doliczany jest czas związany z obsługą uwag Zamawiającego
19.	czas aktualizacji informacji o elemencie konfiguracji w bazie konfiguracji	liczba dni roboczych, która upłynęła od zmiany w elemencie konfiguracji do jej

		wprowadzenia w bazie konfiguracji[1]
20.	poziom aktualności bazy konfiguracji (poziom rozbieżności wykazanych w bazie podczas przeglądu / kontroli konfiguracji względem faktycznego stanu środowisk testowego i produkcyjnego)	wartość procentowa stosunku liczby nieaktualnych elementów konfiguracji w bazie konfiguracji do liczby wszystkich elementów konfiguracji w bazie konfiguracji
21.	częstotliwość przeglądów planów awaryjnych / planów zapewnienia ciągłości	czas który upłynął od poprzedniej realizacji działania
22.	częstotliwość testowania planów awaryjnych / planów zapewnienia ciągłości	czas który upłynął od poprzedniej realizacji działania
23.	procent czynności administracyjnych pokrytych dokumentacją	wartość procentowa stosunku liczby czynności administracyjnych pokrytych dokumentacją do liczby wszystkich czynności administracyjnych
24.	procent parametrów wymaganych objętych monitorowaniem	wartość procentowa stosunku liczby parametrów ujętych w aktualnej koncepcji monitorowania objętych monitorowaniem (weryfikacja na podstawie raportu z monitoringu oraz dodatkowo narzędzi monitorujących) do całkowitej liczby parametrów ujętych w aktualnej koncepcji monitorowania

15 Zasady raportowania realizacji przedmiotu zamówienia

1. Wykonawca w ramach realizacji przedmiotu zamówienia jest zobowiązany do raportowania działań w obszarze utrzymania infrastruktury.
2. Wykonawca będzie raportował z uwzględnieniem:

1) danych z systemów monitorowania (SLA dla obszaru monitorowania),

2) danych z systemów zgłoszeń (SLA dla obszaru utrzymania i serwisu).

3. Wykonawca będzie raportował sposób realizacji usług utrzymania Systemu zgodnie z uzgodnioną procedurą i szablonem raportu poziomu usług, w cyklu miesięcznym w zakresie uzgodnionym z Zamawiającym

15.1 Raportowanie działań w zakresie monitorowania infrastruktury SIG

Wykonawca będzie przygotowywał co najmniej następujące raporty :

1) Standardowe raporty dostępne z
   a) narzędzi do monitorowania HP BSM - do czasu wdrożenia nowych narzędzi monitoringu
   b) dostarczonych narzędzi monitoringu – po ich dostarczeniu
2) Standardowe raporty dostępne poprzez
   a) aplikacje HP SM (service desk) - do czasu wdrożenia nowych narzędzia service desk
   b) dostarczonego narzędzia service desk – po jego dostarczeniu
3) Standardowe raporty dostępne z narzędzi Oracle (dla istniejącego silnika bazy danych)

15.2 Raportowanie usług utrzymania infrastruktury SIG

Wykonawca będzie raportował usługi utrzymania SIG zgodnie z Procedurą raportowania Usług w uzgodnionym szablonie, w cyklu miesięcznym (do 5 dnia roboczego każdego miesiąca). Strony zgodnie z trybem oraz terminami ujętymi w rozdziale 12.5 oraz obowiązującą je Procedurę raportowania Usług Utrzymania infrastruktury rozwiązania SIG oraz szablon Raportu utrzymania i eksploatacji SIG.

15.2.1 Zakres Raportu z utrzymania i eksploatacji infrastruktury

Główną częścią raportu będzie zestawienie wartości dla parametrów wskazanych w rozdziałach 14.1.1 i 14.2.1. Wykonawca jest zobowiązany przedstawić zarówno parametry zagregowane jak i jednostkowe dla poszczególnych elementów infrastruktury, działań i zdarzeń (wyliczane zgodnie z założeniami zawartymi w rozdziałach 14.2.1 oraz 14.2.2). Wykonawca będzie umieszczał w raporcie

rzeczywiste wartości parametrów, tak aby możliwe było ich zweryfikowanie z wartościami wymaganymi. W przypadku wątpliwości Zamawiającego odnośnie wskazanych w raporcie wartości, Wykonawca jest zobowiązany na wezwanie Zamawiającego niezwłocznie udostępnić wszystkie dane źródłowe niezbędne do wyliczenia raportowanych parametrów oraz przedstawić szczegółową metodę ich wyliczania.

Raport utrzymania i eksploatacji SIG będzie ponadto uwzględniał opis realizacji przez Wykonawcę działań związanych z przedmiotem zamówienia, a więc obejmował co najmniej poniższe elementy:

Tabela 18. Zawartość formularza Raportu

Lp.	Element raportu
OBSZAR SERWISU	
1.	Realizacja przyjętych zgłoszeń (w podziale na incydenty, zlecenia standardowe oraz inne zgłoszenia) obejmująca: • wykaz zgłoszeń zarejestrowanych przez Wykonawcę, • wykaz zgłoszeń rozwiązanych przez Wykonawcę, • wykaz zastosowanych obejść w związku z obsługą zgłoszeń, • czasy obsługi dla poszczególnych zgłoszeń; w przypadku przekroczeń w raporcie opisane są okoliczności i przyczyny zaistnienia przekroczeń. Ww. wykazy zostaną umieszczone w raporcie w podziale na wszystkie priorytety zgłoszeń.
2.	Obsługa Problemów: • informacje o wszystkich zarejestrowanych problemach, • wykaz problemów rozwiązanych przez Wykonawcę, • wykaz zastosowanych Obejść w związku z obsługą Problemów, • czasy obsługi dla poszczególnych problemów za ostatni miesiąc; w przypadku przekroczeń w raporcie opisane są okoliczności i przyczyny zaistnienia przekroczeń. Ww. wykazy zostaną umieszczone w raporcie w podziale na wszystkie priorytety problemów.
OBSZAR UTRZYMANIA	
3.	Zarządzanie dostępnością i pojemnością infrastruktury: • **lista sprzętu i licencji** • wykaz zrealizowanych zadań w ramach zarządzanie dostępnością i pojemnością infrastruktury • zestawienie rekomendacji w zakresie planowania dostępnością i pojemnością infrastruktury
4.	Realizacja zmian utrzymaniowych: • wykaz zrealizowanych Zmian utrzymaniowych w Systemie, wraz z informacją o zaktualizowanych dokumentach, • wykaz wycofanych Zmian utrzymaniowych, z podaniem przyczyny ich wycofania.
5.	Zarządzanie konfiguracją: • lista wszystkich elementów konfiguracji,

	• wykaz realizacji działań w ramach zarządzania konfiguracją • zestawienie elementów konfiguracji podlegających zmianom w okresie raportowym wraz ze wskazaniem zmian, które ich dotyczyły
6.	Zarządzanie katalogiem usług: • Lista usług w katalogu usług, • Karty usług.
7.	Zarządzanie ciągłością: • Wykaz realizacji działań w ramach planów zapewniania ciągłości działania systemu
8.	Zarządzanie bezpieczeństwem: • wykaz zrealizowanych zadań w ramach zarządzania bezpieczeństwem, • opis wpływu planowanych i realizowanych Zmian na bezpieczeństwo Systemu, • wynik audytu Systemu pod względem bezpieczeństwa (jeżeli w danym okresie był przeprowadzany).
9.	Wykaz zrealizowanych zadań w ramach zarządzania architekturą
OBSZAR RADY ARCHITEKTURY	
10.	Wykaz zrealizowanych działań w ramach Rady Architektury
REKOMENDACJE	
11.	Wykaz rekomendacji dla Zamawiającego w zakresie utrzymywanej infrastruktury ze szczególnym uwzględnieniem proponowanych zmian

Wykonawca jest zobowiązany do umieszczania w raporcie informacji jednoznacznie wskazujących na realizacje lub nie wymaganych przedmiotem zamówienia działań. W przypadku braku udokumentowania działania lub braku uzasadnienia jego nierealizowania w objętym raportem okresie domyślnie działanie uznawane jest za nierealizowane w okresie raportowym, co będzie podstawą do odrzucenia raportu / lub naliczania kar z powodu braku tego działania.

Wraz z raportem Wykonawca przekazywał wypracowaną dokumentację działań z zakresu utrzymania i eksploatacji infrastruktury SIG.

16 Asysta techniczna

Wykonawca zapewni możliwość skorzystania z usług asysty technicznej. Usługi Asysty technicznej będą świadczone przez Wykonawcę zgodnie z wymaganiami:

1) Wykonawca będzie świadczył na rzecz Zamawiającego usługi związane z np.:
   (1) Obsługą dodatkowych warsztatów nie ujętych w rozdziale 19 Warsztaty;
   (2) Prace o charakterze analitycznym i projektowym;
   (3) Prace związane z administrowaniem, utrzymaniem i konfiguracją dodatkowych systemów pomocniczych wykorzystywanych przez SIG;
   (4) Wsparcie Zamawiającego związane z utrzymaniem usług biznesowych świadczonych przez SIG;
2) Zamawiającemu przysługują usługi asysty technicznej, w wymiarze 10 000 roboczogodzin pracy pracowników Wykonawcy, przez cały okres realizacji przedmiotu zamówienia lub do wykorzystania dostępnych roboczogodzin.
3) Zamawiający będzie zlecał Wykonawcy prace w ramach asysty technicznej w miarę potrzeb;
4) Zastrzega się, że pula godzin może nie zostać w całości wykorzystana. Wykonawcy nie przysługuje z tego tytułu żadne roszczenie odszkodowawcze wobec Zamawiającego;
5) Asysta będzie rozliczana z dokładnością do jednej roboczogodziny. Czas realizacji poszczególnych prac (realizowanych na podstawie odrębnych wniosków Zamawiającego) będzie zaokrąglany w górę z dokładnością do jednej roboczogodziny;
6) Asysta będzie świadczona w siedzibie Zamawiającego lub z miejsca wskazanego przez Zamawiającego, ustalonym z Wykonawcą;
7) Do obliczania wysokości wynagrodzenia dla wykonawcy za świadczenie usługi asysty technicznej stosowana będzie stawka za roboczogodzinę, zgodnie z ceną podaną w ofercie;
8) W ramach usług w zakresie asysty technicznej do Zamawiającego zostanie przypisany dedykowany specjalista Wykonawcy, który będzie odpowiedzialny za realizację usług w zakresie asysty technicznej dla Zamawiającego, a także za przekazywanie oraz otrzymywanie informacji i komentarzy zwrotnych dotyczących świadczonych usług;
9) W przypadku wystąpienia potrzeby skorzystania z asysty Zamawiający skieruje do wykonawcy dokument Wniosek o asystę. Wniosek taki zawierać będzie co najmniej:
   (1) zakres prac do wykonania (ewentualnie opis problemu do rozwiązania),
   (2) określenie proponowanego terminu,
   (3) określenie miejsca wykonania usługi,

10) W terminie nie dłuższym niż 5 dni roboczych od dnia złożenia Wniosku o asystę Wykonawca złoży Zamawiającemu dokument Propozycja asysty. Propozycja taka będzie zawierać co najmniej:
    (1) proponowany zakres prac,
    (2) wykaz pracowników Zamawiającego i wykonawcy, którzy będą uczestniczyli w pracach, wraz z podaniem ich zakresu obowiązków,
    (3) czasochłonność (w roboczogodzinach),
    (4) termin i wymiar godzin realizacji asysty,
11) Wykonawca zrealizuje asystę po otrzymaniu potwierdzenia Propozycji asysty przez Zamawiającego. Nieprzedstawienie Propozycji asysty w terminie 14 dni kalendarzowych będzie traktowane jako zgoda na warunki zawarte we Wniosku o asystę i możliwość realizacji asysty;
12) Po wykonaniu prac i uzyskaniu przez Wykonawcę potwierdzenia ich wykonania przez Zamawiającego, wykonawca przedstawi dokument Raport z asysty, zawierający co najmniej:
    (1) opis wykonanych prac,
    (2) liczbę godzin poświęconych na wykonanie prac,
    (3) całkowitą liczbę godzin asysty zrealizowanych w ciągu trwania asysty, których realizacja została potwierdzona przez Zamawiającego,
13) Realizacja asysty na warunkach innych niż zaproponowane przez Zamawiającego we Wniosku o asystę wymaga zatwierdzenia propozycji Wykonawcy przez Zamawiającego;
14) Wykonawca ma prawo odmówić wykonania asysty o ile:
    (1) Zamawiający wyczerpał przysługujący limit roboczogodzin lub zakończył się okres realizacji umowy,
    (2) realizacja asysty w zaproponowanym zakresie spowodowałaby przekroczenie przysługującego Zamawiającemu limitu roboczogodzin asysty,
    (3) realizacja usług asysty wymagałaby złamania obowiązującego prawa.
15) Zamawiający umożliwi wykonawcy realizację usługi asysty poprzez udostępnienie wymaganych zasobów technicznych oraz niezbędnych pracowników Zamawiającego;
16) W przypadku konieczności zmiany dokumentacji w wyniku wykonania usług asysty wykonawca zobowiązany jest doręczyć zaktualizowaną dokumentację maksymalnie w dwa tygodnie po dostarczeniu przez wykonawcę Raportu z asysty;
17) Po wykonaniu prac asysty technicznej i uzyskaniu przez Wykonawcę potwierdzenia ich Wykonania przez Zamawiającego, Wykonawca przygotuje raport z asysty zawierający co najmniej:
    (1) opis wykonanych prac oraz osiągniętych rezultatów,

(2) liczbę roboczogodzin poświęconych na wykonanie prac,

(3) liczbę roboczogodzin asysty zrealizowanych dotychczas w ramach asysty, których realizacja została potwierdzona przez Zamawiającego.

17 Dokumentacja

W ramach poniższego rozdziału przedstawiono opis dokumentacji, która powinna zostać przekazana przez Wykonawcę w ramach realizacji przedmiotu zamówienia. Terminy przekazywania poszczególnych dokumentacji zostaną ustalone z Wykonawcą w terminie 30 dni od podpisania Umowy.

17.1 Dokumentacja administratora

Dokumentacja administratora powinna obejmować, co najmniej:

- instrukcję instalacji, konfiguracji i administracji dostarczonego oprogramowania,
- opis obsługi codziennej systemu zabezpieczeń,
- opis konfiguracji zastosowanego sprzętu,
- dokumentację zastosowanej instalacji,
- procedury instalacji,
- dokumentację konfiguracji i parametryzacji,
- procedury konfiguracji.

17.2 Dokumentacja projektowa

Dokumentacja projektowa powinna zawierać wszelkie informacje odnośnie zasad prowadzenia projektu. Dokumentacja powinna zawierać co najmniej:

- strukturę projektu,
- plan projektu,
- zasady zarządzania ryzkiem,
- zasady zarządzania jakością,
- zasady zarządzania zmianą w projekcie.

17.3 Dokumentacja powykonawcza

Dokumentacja powykonawcza powinna zawierać co najmniej:

- Projekt funkcjonalny (dotyczy oprogramowania) zawierający m.in.:
  - Model dziedziny (opis modelu dziedziny, diagram modelu dziedziny);
  - Analizę wymagań (lista i opis przypadków użycia);
  - Model funkcjonalny (opis usług aplikacyjnych, tj. komponentów systemów informatycznych, realizujących określone funkcjonalności);
  - Model komunikacji z zewnętrznymi źródłami danych (katalog zewnętrznych źródeł danych, katalog interfejsów);

- Model danych (magazyny systemu gromadzenia danych);
- Model wymagań (katalog wymagań funkcjonalnych oraz poza funkcjonalnych);
- Katalog aktorów (zawiera m.in. określenie realizacji aktorów systemu z usługami aplikacyjnymi).

Dodatkowo: Model wymagań, który można odtworzyć przy użycia narzędzia Enterprise Architect zawierający wymagania składające się z:

- Obowiązkowo – identyfikatora, nazwy, treści wymagania, statusu, stopnia powinności
- Opcjonalnie – powiązania z usługą biznesową, aplikacyjną, danych lub technologiczną, klasyfikacji kontraktu architektonicznego, priorytetu, trudności

- Projekt techniczny (zakres dokumentu opisany we wcześniejszej części niniejszego rozdziału):
  - Analizę dostępnej infrastruktury IT;
  - Opis architektury technologicznej:
    - Metoda opisu;
    - Oprogramowanie aplikacyjne;
    - Infrastruktura oprogramowania;
    - Logiczna infrastruktura sprzętowa:
      - Model infrastruktury maszyn logicznych;
      - Model logicznych woluminów danych;
    - Opis infrastruktury wirtualizacyjnej;
    - Opis fizycznej infrastruktury sprzętowej:
      - Środowisko przetwarzania;
      - Środowisko magazynowania;
    - Opis infrastruktury sieciowej;
    - Opis ośrodków przetwarzania danych oraz infrastruktury telekomunikacyjnej.
- Dokumentacja developerska (dla oprogramowania tworzonego na żądanie), uwzględniająca m.in.
  - Opis kodu źródłowego Systemu;
  - Sposób uruchamiania i kompilacji Systemu;
  - Architekturę kodów źródłowych (diagram obrazujący powiązania pomiędzy plikami Systemu).
- Dokumentacja utrzymaniowa, uwzględniająca m.in.:
  - Sposób monitorowania Systemu;
  - Awarie Systemu:
- Procedury administracyjne – związane z bieżącą eksploatacją oraz przywracania Systemu po awariach

- Dokumentacja instalacji, uwzględniająca m.in.
  - Schemat logiczny Systemu;
  - Konfigurację Systemu;
  - Procedury instalacji Systemu;
  - Procedury odinstalowania Systemu.
- Dokumentacja baz danych, uwzględniająca m.in.
  - Model danych:
    - Model fizyczny baz danych;
    - Opis tabel i kolumn;
    - Relacje;
    - Opisy wyzwalaczy.
- Dokumentacja administratora zawierająca m.in.:
  - Instrukcje dotyczące instalacji;
  - Instrukcje dotyczące konfiguracji;
  - Instrukcje dotyczące administracji;
  - Instrukcje postępowania w przypadkach szczególnych oraz awarii;
  - Opis archiwizacji systemu;
  - Opis zastosowanej konfiguracji i parametryzacji.

17.4 Dokumentacja testów akceptacyjnych

Dokumentacja powinna zawierać wszelkie informacje dotyczące testów akceptacyjnych danego produktów. W skład dokumentacji testów akceptacyjnych mają wchodzić co najmniej:

2. Plany Testów Dopuszczeniowych/Akceptacyjnych uwzględniające m.in.:
   - Zakres testów;
   - Scenariusze testowe;
   - Przypadki testowe;
   - Procedurę zgłaszania błędów;
   - Opis środowiska testowego (konfiguracja środowiska, wykaz niezbędnych zasobów do przeprowadzenia testów);
   - Plan realizacji testów.
3. Raporty z przeprowadzonych Testów Dopuszczeniowych/Akceptacyjnych uwzględniające m.in.:
   - Zakres testów;
   - Wyniki testów;
   - Plan działań następczych związany z wynikami testów.
4. Plany Wdrożeń - Pilotażowe/Masowe, uwzględniające m.in.:

- Przedmiot wdrożenia;
- Plan wdrożenia (odpowiedzialność poszczególnych zasobów, harmonogram i procedury wdrożenia);
- Zasoby niezbędne do przeprowadzenia wdrożenia (zasoby ludzkie i infrastrukturalne);
- Wariant awaryjny.

5. Raporty z Wdrożeń - Pilotażowe/Masowe uwzględniające m.in.:
   - Zakres wdrożenia;
   - Opis przeprowadzonego wdrożenia;
   - Wykaz napotkanych problemów;
   - Działania następcze wynikające z przeprowadzonego wdrożenia.

17.5 Dokumentacja utrzymaniowa

Ogół dokumentacji zawierającej opis procesów oraz procedur związanych z realizacją czynności utrzymaniowych. Dokumentacja powinna obejmować wszystkie procesy realizowane w ramach utrzymania. W ramach dokumentacji utrzymaniowej mają być opracowane m.in.:

- procedury obsługi zgłoszeń,
- procedury ewidencji zgłoszeń serwisowych oraz zdarzeń związanych i ich obsługą,
- analiza wpływu na biznes (ang. *Business Impact Analysis* – BIA),
- szacowanie ryzyka bezpieczeństwa informacji,
- scenariusze planów awaryjnych i planów odtworzeniowych.

18 Odbiór Dokumentacji i Raportów miesięcznych

Dokument/dokumenty (w tym raporty miesięczne) zgłoszone do odbioru zostaną poddane weryfikacji przez Zamawiającego, zgodnie z opisaną poniżej procedurą:

1. Wykonawca przekazuje dokument/dokumenty do odbioru Zamawiającemu wraz z Protokołem Przekazania Dokumentacji w godzinach pracy i w siedzibie Zamawiającego.
2. Zamawiający zapoznaje się z dostarczonym dokumentem/dokumentami w czasie nie dłuższym niż 5 dni roboczych. Jeśli Zamawiający nie zgłasza uwag, to następuje podpisanie Protokołu Odbioru Dokumentu i tym samym zakończenie procedury odbioru dokumentacji. W przeciwnym wypadku Zamawiający rejestruje uwagi w jednolitym Rejestrze Uwag, który przekazuje Wykonawcy i procedura przebiega zgodnie z poniższymi krokami:
    a. W uzgodnionym z Zamawiającym terminie (nie dłuższym niż 3 dni robocze od dnia przekazania uwag), Wykonawca organizuje spotkanie w celu omówienia dostarczonego dokumentu/dokumentów i uwag Zamawiającego
    b. W trakcie spotkania ustalany jest termin (nie dłuższy niż 3 dni robocze) przekazania przez Wykonawcę poprawionego dokumentu/dokumentów zgodnie ze zgłoszonymi i omówionymi podczas spotkania uwagami;
    c. Wykonawca zobowiązany jest przekazać razem z poprawionym dokumentem/ dokumentami Rejestr Uwag, uzupełniony o informacje dotyczące sposobu, w jaki zostały one obsłużone. Zaktualizowany dokument/dokumenty powinien być dostarczony w taki sposób, aby widoczne były w nim naniesione zmiany (np. w trybie „śledzenia zmian”);
    d. Jeżeli Zamawiający ponownie zgłosi uwagi do dokumentu/dokumentów następuje przejście procedury do kroku „a”; Jeżeli Zamawiający nie zgłosi uwag, to następuje Podpisanie Protokołu Odbioru dokumentu i procedura odbioru zostaje zakończona.

W uzasadnionych przypadkach Strony uzgodnią terminy odbiegające od wyżej wymienionych.

W uzasadnionych przypadkach Zamawiający w ustaleniu z Wykonawcą może zrezygnować z przeprowadzenia spotkania o którym mowa w pkt. „a” i „b” procedury.

Dokumentacja będzie dostarczana Zamawiającemu w wersji elektronicznej. Na życzenie Zamawiającego w terminie 3 dni roboczych po dokonaniu odbioru dokumentów Wykonawca dostarczy Zamawiającemu dokumentację w wersji papierowej. Prośba o dostarczenie dokumentacji w formie papierowej powinna zostać zapisana w protokole odbioru dokumentu.

Zamawiający dopuszcza rezygnację z przeprowadzenia ww. procedury dla dokumentów/zapisów dotyczących bieżącego utrzymania rozwiązania– w skład tych dokumentów wchodzą m.in:

- dzienniki administratora,
- rejestr inicjatyw doskonalących/usprawnień,

- raport dla obszaru oprogramowania standardowego,
- plany zarządzania konfiguracją,
- raporty z testów przeglądów planu ciągłości,
- raporty/protokoły z realizacji czynności administracyjnych,
- raporty cząstkowe z monitoringu,

i inne uzgodnione z Zamawiającym po podpisaniu Umowy.

19 Warsztaty

W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany będzie do przeprowadzenia dla Zamawiającego warsztatów z zakresu dostarczonych produktów. Uczestnikami warsztatów będą osoby wskazane przez Zamawiającego. Celem warsztatów będzie samodzielne i optymalne wykorzystywanie dostarczanych przez Wykonawcę rozwiązań. Szczegółowy zakres i harmonogram warsztatów zostanie uzgodniony z Zamawiającym po podpisaniu umowy.

Wymagania w zakresie warsztatów:

1. Warsztaty zostaną przeprowadzone dla 7 osób.
2. Minimalny łączny czas trwania warsztatów musi wynieść 200 godzin.
3. Szczegółowe terminy warsztatów zostaną uzgodnione przez Wykonawcę z Zamawiającym nie później niż 10 dni przed planowanym rozpoczęciem danego warsztatu.
4. Liczba uczestników dla poszczególnych warsztatów będzie zgłaszana przez Zamawiającego najpóźniej 3 dni przed warsztatami.
5. Warsztaty będą odbywać się na terenie m. st. Warszawy.
6. Wykonawca zapewni odpowiednie do przeprowadzenia warsztatów wyposażenie (stacje robocze, sieć, rzutnik, itp.).
7. Wykonawca zapewni uczestnikom warsztatów catering właściwy do czasu trwania warsztatów.
8. Warsztaty będą przeprowadzone w języku polskim.
9. Warsztaty będą prowadzone w formie wykładów i ćwiczeń.
10. Każdy uczestnik warsztatów musi mieć zapewnione samodzielne stanowisko.
11. Przed rozpoczęciem warsztatów Wykonawca zapewni każdemu uczestnikowi komplet materiałów szkoleniowych:
    a. Materiały mają zostać dostarczone w formie papierowej i/lub elektronicznej;
    b. Materiały muszą obejmować całość zagadnień dotyczących zakresu merytorycznego warsztatów;
12. Na zakończenie warsztatów każdy uczestnik otrzyma dokument potwierdzający ich ukończenie.
13. Na zakończenie warsztatów każdy uczestnik wypełnia ankietę, przygotowaną przez Wykonawcę, potwierdzającą zakres i formę warsztatów.
14. Na początku każdego dnia warsztatów Wykonawca sporządzi listę obecności. Udział uczestnika w danym dniu ma zostać potwierdzony jego podpisem.
15. Zamawiający dopuszcza możliwość przeprowadzenie warsztatów poprzez zewnętrzny podmiot.

20 Rola Rady Architektury SIG

Podczas realizacji przedmiotu zamówienia bardzo ważną rolę będzie pełnić Rada Architektury SIG, której podstawowym celem jest wypracowanie oraz rozwijanie, w oparciu o biznesowe cele strategiczne, całościowej wizji architektonicznej Systemów Informatycznych GUGiK. Rada Architektury SIG stanowi ciało decyzyjne w kontekście architektury SIG oraz kształtuje i zatwierdza plany i wizję architektury SIG oraz ustanawia standardy architektoniczne w obrębie Systemów Informatycznych GUGiK.

W skład Rady Architektury SIG wchodzą architekci dziedzinowi będący przedstawicielami wszystkich realizowanych w GUGiK projektów, które są objęte inicjatywą SIG.

Wszystkie prace realizowane przez Wykonawcę muszą być zgodne ze standardami architektonicznymi zatwierdzonymi przez Radę Architektury SIG, a ewentualne uzasadnione odstępstwa od przyjętych standardów muszą być przez nią zatwierdzone.

Zamawiający na potrzeby realizacji Usług będzie przekazywał Wykonawcy obowiązujące wersje standardów SIG.

W przypadku gdy na posiedzeniach Rady Architektury SIG dyskutowane będą zagadnienia architektoniczne związane z rozwiązaniami proponowanymi do implementacji w związku z realizacją Usług, Wykonawca, na wezwanie Zamawiającego, zobowiązany będzie do zapewnienia udziału w spotkaniach architektów rozwiązań, którzy odpowiedzialni będą za przedstawienie zaproponowanych rozwiązań.

Poniżej zakres zadań Wykonawcy w Radzie architektury:

1. tworzenie i aktualizacja architektur cząstkowych w zakresie utrzymania,
2. wsparcie inicjatyw prowadzonych w IT w obszarze utrzymania,
3. tworzenie i komunikowanie standardów i wzorców architektonicznych w obszarze utrzymania,
4. opiniowanie architektur planowanych inicjatyw pod kątem ich późniejszego utrzymania i eksploatacji,
5. wymiarowanie infrastruktury SIG pod planowane bądź rozbudowywane systemy,
6. definiowanie potrzeb infrastrukturalnych,
7. realizacja zadań związanych z zarządzaniem architekturą w obszarze utrzymania stawianych przez Przewodniczącego Rady.

21 Dodatkowe zobowiązania Wykonawcy

Dodatkowe zobowiązania Wykonawcy niewskazane gdzie indziej:

1. Wszelkie działania Wykonawcy w ramach realizacji przedmiotu zamówienia będą oparte o uznane standardy i metodyki wykorzystywane w danym obszarze m.in. ITIL 2011 Edition. Wykonawca będzie realizował przedmiot zamówienia z najwyższą starannością, efektywnością oraz zgodnie z najlepszą praktyką i wiedzą zawodową.
2. Wykonawca zobowiązany jest wykonać w całości przedmiot zamówienia w terminach określonych w niniejszym dokumencie.
3. Wykonawca zobowiązany jest dokonać z Zamawiającym wszelkich koniecznych ustaleń mogących wpływać na przedmiot zamówienia.
4. Wykonawca będzie zobowiązany, w trakcie realizacji umowy, stosować się do wytycznych bezpieczeństwa systemów IT oraz do wytycznych bezpieczeństwa stosowanych u Zamawiającego. Wytyczne zostaną przekazane po podpisaniu umowy.
5. Wykonawca będzie współpracował z Zamawiającym na każdym etapie wykonywania przedmiotu zamówienia w ramach realizacji zamówienia.
6. Wykonawca będzie udzielał Zamawiającemu każdorazowo na wniosek Zamawiającego, pełnej informacji na temat stanu realizacji przedmiotu zamówienia zgodnie z obowiązującą Strony procedurą.
7. Wykonawca będzie współdziałał z osobami wskazanymi przez Zamawiającego. Zamawiający do realizacji powierzonych mu zadań ma prawo desygnować swoich przedstawicieli lub przekazać te zadania do realizacji stronie trzeciej.
8. Wykonawca zobowiązany jest do współpracy z wykonawcami poszczególnych elementów infrastruktury i obszaru aplikacji składającymi się na rozwiązanie w zakresie przejmowania do utrzymania elementów tych systemów. Współpraca te będzie obejmowała w szczególności uczestnictwo w spotkaniach, weryfikację produktów, opracowanie opinii i rekomendacji, uczestnictwo (asystę) w pracach związanych z wprowadzaniem rozwiązań na środowisko produkcyjne.
9. Wykonawca będzie dokumentował działania realizowanie w ramach przedmiotu zamówienia, tj. utrzymywał dokumentację operacyjną związaną ze świadczeniem usług.
10. Wykonawca jest zobowiązany do zapewnienia sobie we własnym zakresie dodatkowych narzędzi do monitorowania systemów / infrastruktury programowo-sprzętowej inne niż będące w posiadaniu Zamawiającego, w przypadku gdy uzna je za niezbędne do realizacji przedmiotu zamówienia. Wykonawca przed włączeniem ww. narzędzi do środowiska monitoringu uzyska akceptację Zamawiającego w tym zakresie. Wykonawca będzie również rekomendował zmiany w zakresie realizowanego monitoringu infrastruktury programowo-sprzętowej Zamawiającemu.
11. Wszelkie dane i informacje wytwarzane przez Wykonawcę i utrzymywane w ramach realizacji przedmiotu zamówienia są własnością Zamawiającego (dotyczy to w szczególności danych i informacji gromadzonych w narzędziach monitorujących, także dodatkowo zapewnianych przez Wykonawcę). Wykonawca zobowiązany jest do przekazania Zamawiającemu wszystkich

danych i informacji oraz dokumentów wytwarzanych i gromadzonych w ramach realizacji przedmiotu zamówienia po zakończeniu umowy. Wykonawca jest zobowiązany do zachowania poufności wszystkich danych i informacji, w których posiadanie wejdzie podczas realizacji przedmiotu Umowy.

12. Wykonawca umożliwi Zamawiającemu, lub wskazanemu przez niego podmiotowi, realizację audytów jakości wykonania przedmiotu zamówienia. Z wykonania audytu Zamawiający sporządzi na piśmie protokół zaleceń poaudytowych i przekaże go Wykonawcy. Wykonawca zobowiązany jest do wprowadzenia zaleceń poaudytowych wykazujących niezgodności w realizacji przez Wykonawcę Umowy. Wprowadzenie ww. zaleceń poaudytowych nastąpi w terminie uzgodnionym przez Strony.
13. Wykonawca umożliwi Zamawiającemu, lub wskazanemu przez niego podmiotowi, prowadzenie kontroli wykonania działań w ramach przedmiotu Umowy. Po wykonania kontroli Zamawiający sporządzi na piśmie raport z wnioskami pokontrolnymi i przekaże go Wykonawcy. Wyniki kontroli będą miały wpływ na dalsze działania związane z zarządzaniem umową z Wykonawcą.

22 Dodatkowe zobowiązania Zamawiającego

Dodatkowe zobowiązania Zamawiającego niewskazane gdzie indziej:

1. Udostępnienie dokumentów, materiałów, danych, dokumentacji i informacji będących w posiadaniu Zamawiającego, niezbędnych do realizacji przedmiotu zamówienia.
2. Udzielanie Wykonawcy na bieżąco niezbędnych do realizacji przedmiotu zamówienia wyjaśnień oraz przekazywania niezbędnych informacji.
3. Informowanie Wykonawcy o wszelkich czynnościach podejmowanych w związku z realizacją projektu, jeśli będą one miały związek z realizacją przedmiotu zamówienia przez Wykonawcę.
4. Umożliwienie Wykonawcy dostępu do posiadanych przez Zamawiającego obiektów, sprzętu, oprogramowania oraz dokumentacji, niezbędnych do realizacji przedmiotu zamówienia, zgodnie z wewnętrznymi regulacjami Zamawiającego w zakresie bezpieczeństwa.
5. Prowadzenie biura projektu, w tym prowadzenie repozytorium dokumentacji.

23 Załączniki

Załącznik numer 1 - Architektura SIG

Załącznik numer 2 – Studium wykonalności projektu CAPAP

Załącznik numer 3 – Studium wykonalności projektu ZSIN Faza II

Załącznik numer 4 – Studium wykonalności projektu K-GESUT

Załącznik numer 5 - Protokół Odbioru Ilościowego