

Opis przedmiotu zamówienia:

Świadczenie usług utrzymania, gwarancji, serwisu i usług rozwoju systemu Platforma Lokalizacyjno-Informacyjna z Centralną Bazą Danych (PLI CBD) oraz dostawa sprzętu i oprogramowania wraz z instalacją, skonfigurowaniem, uruchomieniem i integracją sprzętu i oprogramowania z Aplikacją PLI CBD i Infrastrukturą Informatyczną PLI CBD

Spis treści

1.	Przedmiot zamówienia	3
1.1	Płatności	3
1.2	Harmonogram	3
2.	Definicje	4
3.	Opis ogólny całego rozwiązania	13
3.1	Środowisko aplikacyjne PLI CBD	14
3.2	Środowisko sprzętowe IT	15
3.3	Opis Infrastruktury Technicznej	18
4.	Zasady współpracy Wykonawcy z Zamawiającym	19
4.1	Wdrożenie sprzętu i oprogramowania do Systemu PLI CBD	19
4.2	Zatrzymanie Systemu PLI CBD	20
4.3	Zarządzanie zmianą	20
5.	Wymagania ogólne na usługi utrzymania	20
6.	Wymagania ogólne na usługi rozwoju	23
7.	Wymagania w zakresie przetwarzania danych osobowych	24
8.	Wymagania ogólne na usługi gwarancji	25
9.	Wymagania ogólne na usługi wdrożeniowe	28
10.	Wymagania pozafunkcjonalne	29
11.	Wymagania na utrzymanie środowiska serwerowego SRV	34
12.	Wymagania na rozwój środowiska serwerowego SRV	39
13.	Wymagania na utrzymanie środowiska sieciowego LAN	46
14.	Wymagania na rozwój środowiska sieciowego LAN	48
15.	Wymagania na utrzymanie środowiska bazodanowego BD	56
16.	Wymagania na utrzymanie Aplikacji PLI CBD	58
17.	Wymagania na rozwój Aplikacji PLI CBD	61

Załącznik A. Opis środowiska serwerowego SRV

Załącznik B. Zestawienie sprzętu serwerowego i oprogramowania

Załącznik C. Mapowanie licencji środowiska serwerowego

Załącznik D. Opis środowiska sieciowego LAN

Załącznik E. Zestawienie sprzętu sieciowego i oprogramowania

Załącznik F. Opis środowiska bazodanowego BD

Załącznik G. Zestawienie serwisów i usług Aplikacji PLI CBD

Załącznik H. Opis środowiska Systemu Obsługi Użytkowników SOU

1. Przedmiot zamówienia

Przedmiotem umowy jest świadczenie usług utrzymania, gwarancji, serwisu i usług rozwoju systemu Platforma Lokalizacyjno-Informacyjna z Centralną Bazą Danych (PLI CBD) oraz dostawa sprzętu i oprogramowania wraz z instalacją, skonfigurowaniem, uruchomieniem i integracją sprzętu i oprogramowania z Aplikacją PLI CBD i Infrastrukturą Informatyczną PLI CBD.

Miejszem realizacji tego zadania są Centra Przetwarzania Danych Platformy Lokalizacyjno-Informacyjnej z Centralną Bazą Danych (CPD PLI CBD) zlokalizowane w Boruczy (ok. 50 km od Warszawy) i w Siemianowicach Śląskich oraz w Centrali UKE w Warszawie. W ramach umowy Wykonawca zakupi, dostarczy, wymieni i skonfiguruje komponenty Systemu PLI CBD wyszczególnione w wymaganiach, na które udzieli gwarancji i będzie świadczył usługi utrzymania i serwisu. Komponenty te wejdą automatycznie w obszar zdefiniowany jako Aplikacja PLI CBD lub Infrastruktura Informatyczna PLI CBD, a wymienione komponenty (zastąpione komponenty) automatycznie po procesie wymiany zostaną z tych obszarów definicji usunięte.

Celem zamówienia jest utrzymanie, wsparcie, wdrożenie, rozwój Systemu PLI CBD oraz dostawa sprzętu i oprogramowania. Wymagać będzie to od Wykonawcy:

- 1) dostawy i wdrożenia sprzętu oraz dostarczenia oprogramowania niezbędnego do realizacji przedmiotu Umowy oraz przeniesienia autorskich praw majątkowych do dokumentacji wytworzonej w ramach realizacji Umowy, Oprogramowania Dedykowanego, kodów źródłowych oprogramowania dedykowanego, produktów wykonanych w ramach realizacji Umowy, w tym świadczenia usług serwisu gwarancyjnego, jak również na udzieleniu Zamawiającemu licencji niezbędnych do realizacji przedmiotu Umowy,
- 2) udzielenia Zamawiającemu gwarancji na System PLI CBD, na zasadach określonych w niniejszym dokumencie, w tym na wytworzone/dostarczone nowe funkcjonalności oraz na funkcjonalności oraz komponenty, które uległy modyfikacji, w tym powstałe w wyniku dokonania zmian Systemu PLI CBD, świadczenie serwisu gwarancyjnego na System PLI CBD,
- 3) wykonywania usług rozwojowych i wdrożeniowych Systemu PLI CBD.

1.1 Płatności

Szczegółowe zapisy dotyczące płatności za realizację opisanych usług, w tym również dostaw i wdrożenia sprzętu zapisane będą w umowie.

1.2 Harmonogram

Realizacja przedmiotu zamówienia będzie przebiegała zgodnie z Harmonogramem przygotowanym przez Wykonawcę i zatwierdzonym przez Zamawiającego.

Wykonawca, sporządzając propozycję Harmonogramu, musi brać pod uwagę:

- zależności pomiędzy realizowanymi wymaganiami, tak, aby skutki realizacji wymagania nie były ograniczone w wyniku niezrealizowania innego, powiązanego wymagania,
- optymalizację doboru działań, tak, aby podobne prace (np. konfigurowanie systemów) nie musiały być realizowane wielokrotnie,
- konieczność zachowania ciągłości funkcjonowania Systemu PLI CBD,
- dostępność personelu Zamawiającego powodująca konieczność rozłożenia niektórych działań w czasie,
- wymagania w zakresie prac serwisowych (w tym przeglądów),

- potrzebę wprowadzenia zmian prawnych.

Harmonogram musi uwzględniać wszystkie prace wymagane do realizacji wymagań opisanych w kolejnych rozdziałach. **Termin wykonania zamówienia:**

1. Wykonawca realizował będzie zamówienie w zakresie usługi utrzymania, gwarancji, serwisu, usług rozwoju oraz w zakresie dostawy i wdrożenia sprzętu wraz z migracją konfiguracji, przez okres **12 miesięcy** od daty zawarcia umowy.

2. Definicje

Pojęcie	Definicja
System PLI CBD (System)	System Platforma Lokalizacyjno-Informacyjna z Centralną Bazą Danych (PLI CBD) to System Informatyczny, o którym mowa w art. 78 ust. 4 ustawy Prawo telekomunikacyjne. System PLI CBD składa się z Aplikacji PLI CBD, Infrastruktury Informatycznej PLI CBD oraz Infrastruktury Technicznej PLI CBD. Systemem PLI CBD zarządza Prezes UKE na podstawie art. 78 ust. 6 ustawy Prawo telekomunikacyjne. System PLI CBD został wytworzony podczas dwóch projektów, które zostały zakończone odpowiednio w czerwcu 2011 roku oraz w czerwcu 2015 roku i pojęciem System PLI CBD określane są rezultaty i produkty obu tych projektów. Systemem PLI CBD są również modernizacje Aplikacji jak i Infrastruktury Informatycznej dokonane w ramach umów utrzymaniowych realizowanych w latach 2017-2024.
E112	Usługa lokalizacyjno-informacyjna.
Usługi wdrożeniowe	Opisane w dokumentacji działania mające na celu wdrożenie do produkcji i integrację nowych rozwiązań z Systemem PLI CBD.
Aplikacja PLI CBD	Oprogramowanie, w skład którego wchodzi: <ol style="list-style-type: none"> 1. zasadnicze rozwiązania funkcjonalne Systemu PLI CBD zapewniające świadczenie usług: <ul style="list-style-type: none"> • lokalizacyjnych E112 (ang. <i>Emergency</i>) dla zgłoszeń ratunkowych, • przenośności numeru NP (ang. <i>Number Portability</i>), • Centralnej Bazy Danych numerów przeniesionych CBD (ang. <i>Central Database</i>), tzn.: Oprogramowanie Dedykowane Aplikacji Platformy Lokalizacyjno-Informacyjnej z Centralną Bazą Danych (PLI CBD); Oprogramowanie Dedykowane Systemowi Obsługi Użytkowników (SOU); Standardowe Oprogramowanie Aplikacyjne (systemy zarządzania bazami danych, systemy kopii zapasowych (<i>backup</i>); serwery Aplikacji PLI CBD i serwery bazodanowe; procedury w bazach danych, usługi sieciowe (ang. <i>web service</i>), usługi, skrypty itp., <ol style="list-style-type: none"> 2. pomocnicze rozwiązania infrastrukturalne, tzn. serwery www, serwery DNS, System poczty elektronicznej MS Exchange i inne); Standardowe Oprogramowanie Systemowe (systemy operacyjne Microsoft Windows Server i Linux), systemy odpowiedzialne za bezpieczeństwo i komunikację pomiędzy Centrami Przetwarzania Danych (CPD) oraz

Pojęcie	Definicja
	<p>między Centrami Przetwarzania Danych a systemami operatorów telekomunikacyjnych oraz służb.</p> <p>W skład Aplikacji PLI CBD wchodzi również systemy wspierające System PLI CBD takie jak system monitoringu Aplikacji PLI CBD. Aplikacja PLI CBD zainstalowana została na Infrastrukturze Informatycznej PLI CBD zarówno na środowisku testowym, jak i produkcyjnym we wszystkich lokalizacjach, tzn.: dwa CPD PLI CBD oraz Centrala UKE. W skład Aplikacji PLI CBD wchodzi Komponenty Zastanej Aplikacji PLI CBD szczegółowo wymienione w załącznikach do niniejszego dokumentu jak i oprogramowania dodane, wymienione lub uzupełnione w ramach realizacji niniejszej umowy. Aplikacja PLI CBD zainstalowana jest na środowisku produkcyjnym oraz środowisku testowym.</p>
Infrastruktura Informatyczna	<p>To środowisko sprzętowe, na którym zainstalowana jest Aplikacja PLI CBD składnikami tego środowiska są: serwery, komputery stacjonarne, komputery przenośne (laptop/notebook), macierze dysków, urządzenia sieciowe, takie jak routery, przełączniki, urządzenia równoważenia obciążenia (<i>load balancer</i>), zapory sieciowe (<i>firewall</i>) i inne, urządzenia systemu kopii zapasowych (<i>backup</i>) oraz nośniki przechowujące kopie zapasowe danych (<i>backup</i>), biblioteki taśmowe oraz taśmy wchodzące w ich wyposażenie, skanery, drukarki, aparaty telefoniczne VoIP (Cisco), monitory wchodzące w skład serwerów i komputerów PC, wielkoformatowe monitory LCD, jak i telewizory/monitory LCD. Infrastruktura Informatyczna PLI CBD obejmuje całość sprzętu informatycznego IT dostarczonego w ramach prowadzonych dwóch projektów: PLI CBD i PLI CBD2 oraz innych umów na utrzymanie i rozwój. W skład Infrastruktury Informatycznej PLI CBD wchodzi Komponenty Zastanej Infrastruktury Informatycznej PLI CBD szczegółowo wymienionej w załącznikach do niniejszego dokumentu, jak również elementy dodane, wymienione lub uzupełnione w ramach realizacji niniejszej umowy. Integralnym elementem Infrastruktury Informatycznej jest również środowisko testowe znajdujące się w Centrum Przetwarzania Danych PLI CBD. Elementy tej infrastruktury są przedmiotem niniejszej umowy.</p>
Infrastruktura Techniczna	<p>Całość sprzętu znajdującego się w Centrach Przetwarzania Danych PLI CBD dostarczona i zainstalowana w ramach prowadzonych dwóch projektów PLI CBD oraz PLI CBD2, a nie wymieniona w pozycji Infrastruktura Informatyczna PLI CBD wraz z systemem jej monitoringu oraz wykorzystywanym przez tę infrastrukturę oprogramowaniem. W skład Infrastruktury Technicznej PLI CBD wchodzi Komponenty Zastanej Infrastruktury Technicznej PLI CBD szczegółowo wymienionej w załącznikach do niniejszego dokumentu, jak również elementy dodane, wymienione, uzupełnione w ramach realizacji niniejszej umowy oraz także dodane, wymienione lub uzupełnione w czasie trwania niniejszej umowy. Elementy tej infrastruktury nie są przedmiotem niniejszej umowy.</p>
Usługi Utrzymania	<p>Opisane Umową usługi mające na celu zapewnienie poprawnego działania Systemu PLI CBD oraz wsparcie Zamawiającego w korzystaniu z Systemu</p>

Pojęcie	Definicja
	PLI CBD. W ramach usługi utrzymania Systemu PLI CBD Wykonawca zobowiązany będzie do naprawy Błędów Systemu PLI CBD wynikłych w trakcie jego użytkowania, naprawy (usuwania) Błędów/Awarii Aplikacji PLI CBD oraz sprzętu wchodzącego w skład Infrastruktury Informatycznej PLI CBD.
Usługi Rozwoju	Opisane Umową usługi mające na celu zapewnienie modyfikacji i rozbudowy Systemu PLI CBD. Usługi rozwoju w ramach Systemu PLI CBD dotyczą zarówno Aplikacji PLI CBD, jak i Infrastruktury Informatycznej PLI CBD. W ramach usług realizowane będą zadania wynikające np. ze zmian prawnych wpływających na konieczność modyfikacji Aplikacji PLI CBD, dodatkowych funkcjonalności opisanych w OPZ lub modyfikacji funkcjonalności już zrealizowanych w ramach projektów PLI CBD i PLI CBD2. W ramach Usługi Rozwoju dokonywane będą również wymiany Komponentów Infrastruktury Informatycznej PLI CBD. Na wykonane prace w ramach Usług Rozwoju Wykonawca udziela usługi gwarancji i usługi utrzymania oraz usługi serwisu.
Usługi Serwisu	Opisane Umową usługi dotyczą całego Systemu PLI CBD i tych jego Komponentów, które wymagają okresowych przeglądów (z uwzględnieniem warunków wynikających z ich instalacji, a także wymagań wynikających z zaleceń producentów dla poszczególnych systemów i urządzeń), wymiany elementów eksploatacyjnych w zakresie Infrastruktury Informatycznej PLI CBD, ale również przeglądów związanych z Aplikacją PLI CBD, np. w sferze jej wydajności, czyszczenia niepotrzebnych plików zdarzeń log i optymalizacji konfiguracyjnej zarówno Aplikacji PLI CBD, jak i elementów Infrastruktury Informatycznej PLI CBD.
Usługi Gwarancji	Opisane Umową usługi dotyczą całego Systemu PLI CBD oraz obejmują również te Komponenty, które w ramach pozostałych usług (utrzymania, rozwoju, serwisu) zostały wymienione na nowe lub uzupełnione o nowe elementy. Działania gwarancyjne mają zapewnić zachowanie cech określonych w specyfikacjach.
Gwarancja	Udzielona przez Wykonawcę, w ramach wynagrodzenia, gwarancja poprawnego funkcjonowania Systemu PLI CBD, w ramach której Wykonawca zobowiązany jest do usuwania Błędów, Awarii w Systemie PLI CBD na warunkach oraz w zakresie wskazanym w Umowie.
Akceptacja	Odbiór Produktu/Usługi/Naprawy awarii lub błędu – przegląd jakości pod względem merytorycznym przeprowadzony przez specjalistów – administratorów z PLI CBD , dla której/którego wykonywany jest Produkt/Usługa/Naprawa awarii lub błędu, dokonywana zgodnie z procedurą opisaną w Umowie zakończona podpisaniem Protokołu.
Aktualizacja	Dostarczenie i wdrożenie standardowego, dostarczonego przez producenta oprogramowania składającego się na System PLI CBD (w tym również przez Wykonawcę w części, w jakiej Wykonawca jest producentem

Pojęcie	Definicja
	oprogramowania składającego się na System PLI CBD), uaktualnienie Systemu PLI CBD w ramach jego wersji głównej, służące do usunięcia stwierdzonych nieprawidłowości pracy Systemu PLI CBD, dodanie standardowych nowych funkcjonalności lub uwzględnienie zmian w powszechnie obowiązujących przepisach prawa.
Błędy/Awarie (definicja ogólna)	<p>Każda nieprawidłowość w funkcjonowaniu Systemu PLI CBD lub Infrastruktury Informatycznej stwierdzona przez Zamawiającego lub niezgodna z wymaganiami tego dokumentu powodująca niemożność lub utrudnienia w eksploatacji Systemu PLI CBD lub Infrastruktury Informatycznej.</p> <p>Każda nieprawidłowość w działaniu Komponentu Systemu PLI CBD, niezależnie od przyczyny takiej nieprawidłowości.</p> <p>Błędy/Awarie dzielą się na cztery poniższe kategorie:</p> <ul style="list-style-type: none"> - Błędy/Awarie Krytyczne, - Błędy/Awarie Poważne, - Błędy/Awarie, - Błędy/Awarie niskiej kategorii.
Błąd/Awaria Krytyczna	<p>Nieprawidłowe działanie Komponentu Systemu PLI CBD powodujące brak możliwości korzystania z Aplikacji PLI CBD, albo takie ograniczenie możliwości korzystania z niej, że przestaje ona spełniać swoje funkcje, powodując zatrzymanie lub opóźnienia w przebiegu procesów biznesowych realizowanych przez Zamawiającego określonych w zatwierdzonej przez niego Dokumentacji Systemu PLI CBD. Przykładem Błędu Krytycznego jest niemożność uruchomienia Aplikacji PLI CBD, brak odczytu/zapisu z bazy danych, utrata danych lub ich spójności, brak możliwości zalogowania użytkownika, niedostępność krytycznych funkcji Aplikacji PLI CBD, a także brak dostępności którejkolwiek z usług:</p> <ul style="list-style-type: none"> • lokalizacyjnych E112 dla zgłoszeń ratunkowych, • przenośności numeru NP, • centralnej bazy numerów przeniesionych, <p>realizowanych przez Oprogramowanie Dedykowane w Aplikacji PLI CBD, polegające na braku odbierania lub wysyłania komunikatów.</p> <p>Oznacza awarię, w której oprogramowanie:</p> <p>a) jakkolwiek z oferowanych przez System PLI CBD usługa nie funkcjonuje, w szczególności dotyczy to usług związanych z lokalizacją abonenta lub z przenoszeniem numerów, niezależnie od przyczyny takiej awarii,</p> <p>lub</p> <p>b) uniemożliwia prawidłowe (to jest także w wymaganym czasie) wykonywanie istotnych dla użytkownika operacji w oprogramowaniu (w</p>

Pojęcie	Definicja
	<p>tym krytycznych czasowo), powodując zatrzymanie lub istotne opóźnienia w procesach biznesowych realizowanych przez Zamawiającego określonych w zatwierdzonej przez niego dokumentacji oprogramowania (Systemu PLI CBD), co do którego nie istnieje skuteczne obejście.</p> <p>Czas skutecznej naprawy Błędu/Awarii krytycznej wynosi do 72 godzin od momentu zgłoszenia przez Zamawiającego.</p> <p>Czasy realizacji zgłoszenia Błędu/Awarii krytycznej określono w wymaganiu G-WSP-011.</p>
Błąd/Awaria Poważna	<p>Nieprawidłowe działanie Komponentu Systemu PLI CBD powodujące ograniczenie korzystania z Aplikacji PLI CBD przy zachowaniu spełniania przez Aplikację PLI CBD jej podstawowych funkcji. Przykładem Błędu Poważnego jest niedostępność niekrytycznych funkcji Aplikacji PLI CBD (np. aplikacja SOU) czy wydajność poniżej określonego progu itp. Błędem Poważnym jest również nieprawidłowe działanie któregośkolwiek z elementów Infrastruktury Informatycznej wymienionego w załączniku:</p> <ul style="list-style-type: none"> • Załącznik B. Zestawienie sprzętu serwerowego i oprogramowania • Załącznik C. Mapowanie licencji środowiska serwerowego • Załącznik E. Zestawienie sprzętu sieciowego i oprogramowania <p>Czas skutecznej naprawy Błędu/Awarii poważnej wynosi do 96 godzin od momentu zgłoszenia przez Zamawiającego.</p> <p>Czasy realizacji zgłoszenia Błędu/Awarii poważnej określono w wymaganiu G-WSP-011.</p>
Błąd/Awaria	<p>Błąd/Awaria może dotyczyć niektórych zgłoszeń nieprawidłowości w działaniu Systemu PLI CBD zgłaszanych przez podmioty zewnętrzne takie jak Przedsiębiorcy Telekomunikacyjni lub służby.</p> <p>Czas skutecznej naprawy Błędu/Awarii wynosi do 30 dni od momentu zgłoszenia przez Zamawiającego.</p> <p>Czasy realizacji zgłoszenia Błędu/Awarii określono w wymaganiu G-WSP-011.</p>
Błąd/Awaria Niskiej Kategorii	<p>Nieprawidłowe działanie Komponentu Systemu PLI CBD niepowodujące ograniczenia korzystania z Aplikacji PLI CBD, które skutkuje jedynie niedogodnościami w zakresie eksploatacji Systemu PLI CBD. Przykładem Błędu Niskiej Kategorii jest np. uszkodzenie komputera stacjonarnego, drukarki albo błąd językowy w interfejsie użytkownika.</p> <p>Oznacza awarię niepowodującą zatrzymania lub istotnych opóźnień w procesach biznesowych realizowanych przez Zamawiającego określonych w zatwierdzonej przez niego dokumentacji oprogramowania (Systemu PLI CBD), co do którego istnieje skuteczne obejście.</p>

Pojęcie	Definicja
	<p>Czas skutecznej naprawy Błędu/Awarii niskiej kategorii wynosi do 30 dni od momentu zgłoszenia przez Zamawiającego.</p> <p>Czasy realizacji zgłoszenia Błędu/Awarii niskiej kategorii określono w wymaganiu G-WSP-011.</p>
Oprogramowanie	Całość lub dowolny element Oprogramowania dostarczonego lub wykonanego w ramach realizacji umów na budowę Systemu PLI CBD (środowisko zastane) oraz niniejszej umowy.
Standardowe Oprogramowanie Systemowe	Oprogramowanie tworzące środowisko, w którym uruchamiane jest Oprogramowanie, w tym oprogramowanie systemowe lub bazodanowe. Standardowe Oprogramowanie Systemowe jest wymienione w : Załączniku A. Opis środowiska serwerowego SRV, Załączniku B. Zestawienie sprzętu serwerowego i oprogramowania oraz Załączniku C. Mapowanie licencji środowiska serwerowego.
Standardowe Oprogramowanie Aplikacyjne	Oprogramowanie będące podstawą do stworzenia Systemu PLI CBD, istniejące i dystrybuowane przed zawarciem umowy. Standardowe Oprogramowanie Aplikacyjne jest wymienione w Załączniku G. Zestawienie serwisów i usług Aplikacji PLI CBD.
Oprogramowanie Dedykowane	Oprogramowanie tworzone na potrzeby umowy, w tym rozbudowa lub modyfikacja Standardowego Oprogramowania Aplikacyjnego. Jeżeli dane Oprogramowanie nie zostało przypisane do Standardowego Oprogramowania Systemowego lub Standardowego Oprogramowania Aplikacyjnego uważa się je za Oprogramowanie Dedykowane.
Materiały Dedykowane	Rezultaty prac (w tym utwory w rozumieniu przepisów ustawy o prawie autorskim i prawach pokrewnych), które zostały stworzone lub dostarczone przez Wykonawcę na potrzeby lub w ramach realizacji umowy, zarówno w postaci elektronicznej, jak i papierowej, a które nie stanowią Oprogramowania.
Oprogramowanie Open Source	Oprogramowanie dystrybuowane na warunkach tzw. licencji otwartych.
Podwykonawca	Podmiot, któremu Wykonawca powierzy wykonanie części swoich zobowiązań wynikających z umowy.
Umowa SLA	Postanowienia umowy określające zasady usuwania Błędów, Awarii lub parametry jakościowe dotyczące działania Systemu PLI CBD.
Dostępność Systemu PLI CBD	Oznacza stopień możliwości korzystania z pełnej funkcjonalności oprogramowania przez użytkowników Systemu PLI CBD.
Eksploatacja	Czynności realizowane w ramach używania Systemu PLI CBD. Obejmują zarówno kwestie administracyjne (np. backup, przydzielanie uprawnień), jak i korzystanie z funkcji Systemu PLI CBD – zarówno przez administratorów, jak i użytkowników.

Pojęcie	Definicja
Czas Reakcji	<p>Czas między zgłoszeniem Błędu/Awarii a uzyskaniem potwierdzenia przystąpienia do jego usunięcia.</p> <p>Oznacza czas, w którym personel Wykonawcy przystępuje do pracy nad rozwiązaniem problemu przez potwierdzenie przyjęcia zgłoszenia serwisowego zgodnie z opisem niniejszego opracowania. W ramach czasu reakcji Wykonawca wspólnie z Zamawiającym dokona zbadania kompletności zgłoszenia, uzupełnienia informacji, weryfikacji klasyfikacji problemu oraz potwierdzi przyjęcie problemu do rozwiązania.</p>
Czas skutecznej Naprawy	<p>Czas między zgłoszeniem Błędu/Awarii a jego usunięciem.</p> <p>Oznacza czas, w którym Wykonawca zobowiązany jest do usunięcia nieprawidłowości.</p>
Incydent	<p>Każde zdarzenie, które nie jest częścią standardowego działania Systemu PLI CBD, a także nieplanowana przerwa w usłudze gwarancyjnej świadczonej przez Wykonawcę.</p>
Naprawa	<p>Usunięcie przez Wykonawcę Błędu, Awarii w szczególności poprzez dokonanie zmian w konfiguracji, kodzie lub architekturze Systemu PLI CBD, w tym przywrócenie prawidłowego funkcjonowania Aplikacji PLI CBD oraz Infrastruktury Informatycznej.</p>
Niezawodność Systemu PLI CBD	<p>Oznacza docelową niezawodność Systemu PLI CBD wykazującego co najwyżej 1 nieplanowane zatrzymanie Systemu PLI CBD w danym okresie rozliczeniowym w czasie gotowości serwisowej.</p>
Obejście	<p>Przywrócenie działania Systemu PLI CBD do stanu sprzed wystąpienia Błędu/Awarii z możliwymi ograniczeniami efektywnościowymi korzystania z Systemu PLI CBD, nie uniemożliwiającymi jednak realizacji usług i funkcji obsługiwanych przez System PLI CBD. Obejście nie stanowi usunięcia Błędu/Awarii.</p>
Wsparcie techniczne	<p>Czynności realizowane przez Wykonawcę polegające na rozwiązywaniu problemów i udzielaniu rozwiązań lub odpowiedzi na problemy zgłaszane przez administratorów systemu PLI CBD, a dotyczących błędnie funkcjonującego oprogramowania systemowego, bazodanowego i specjalistycznego (oprogramowanie monitorujące, backupowe, oprogramowanie macierzy i urządzeń sieciowych) wykorzystywanego w PLI CBD. Wsparcie techniczne dotyczy również problemów zgłaszanych przez administratorów systemu PLI CBD związanych z błędnie funkcjonującym sprzętem, na którym to oprogramowanie jest zainstalowane. Czas rozwiązania problemu i udzielenia przez Wykonawcę odpowiedzi powinien być dostosowany do zagrożenia typem awarii, która może być konsekwencją zgłaszanego problemu lub błędu. W przypadku problemu, którego brak rozwiązania może być zagrożony niedostępnością systemu PLI CBD - czas udzielenia odpowiedzi powinien być taki, by zagwarantowany został czas przywrócenia dostępności systemu zgodny z tabelą znajdującą się w przedmiotowym załączniku – identyfikator G-WSP-</p>

Pojęcie	Definicja
	011. W przypadku braku takiego zagrożenia czas rozwiązania problemu i udzielenia odpowiedzi powinien być identyczny jak czas obsługi Błędu/Awarii Poważnego przez Wykonawcę w Systemie PLI CBD.
Zatrzymanie Systemu PLI CBD	Oznacza brak dostępności Systemu PLI CBD uniemożliwiający Zamawiającemu świadczenie którychkolwiek usług na rzecz klientów.
Zgłoszenie masowe	Wielokrotne zgłoszenie dotyczące tego samego problemu.
Odbiór	<p>Czynności mające na celu potwierdzenie dostarczenia oraz prawidłowego wykonania Produktów/Usług wykonanych w ramach realizacji niniejszej Umowy, w szczególności dostarczenia komponentów Systemu PLI CBD, dokumentacji oraz naprawy Błędów/Awarii zgodnie z postanowieniami Umowy, na zasadach określonych w Umowie. Z czynności Odbioru sporządza się Protokół Odbioru, w którym stwierdza się, między innymi, potwierdzenie dostarczenia Produktów, zgodnie z postanowieniami Umowy albo wskazuje się Błędy/Awarie lub inne nieprawidłowości.</p> <p>Czynności mające na celu potwierdzenie, że dostawa Produktu/Usługi/Naprawa awarii lub błędu zawiera wszystkie wymagane elementy.</p> <p>Czynności mające na celu potwierdzenie, że Wykonawca spełnił wszystkie wymagania dla wykonania danego Produktu/Usługi/Naprawy awarii lub błędu zakończony podpisaniem Protokołu Odbioru Produktu/Usługi/Naprawy awarii lub błędu bez zastrzeżeń.</p> <p>Czynności mające na celu potwierdzenie, że Produkt/Usługa/Naprawy awarii lub błędu spełnia wymagania jakościowe. Odbiór zakończony jest podpisaniem Protokołu Odbioru.</p>
Testy	Proces wykonywany przez Wykonawcę z wykorzystaniem środowiska testowego przy wsparciu Zamawiającego, celem weryfikacji i formalnego potwierdzenia zgodności funkcjonalności testowanego komponentu Systemu PLI CBD z wymaganiami zawartymi w Umowie pomiędzy Zamawiającym a Wykonawcą. W szczególności dotyczy to przeprowadzania testów regresyjnych po dokonaniu modyfikacji, poprawieniu błędów lub po dodaniu nowej funkcjonalności w Systemie PLI CBD.
Zastana Aplikacja PLI CBD	Stan zasobów Aplikacji PLI CBD na dzień podpisania umowy wyszczególniony w Załączniku G. Zestawienie serwisów i usług Aplikacji PLI CBD do niniejszego dokumentu.
Zastana Infrastruktura Informatyczna	<p>Stan zasobów Infrastruktury Informatycznej na dzień podpisania umowy wyszczególniono w:</p> <ul style="list-style-type: none"> - Załącznik A. Opis środowiska serwerowego SRV - Załącznik B. Zestawienie sprzętu serwerowego i oprogramowania - Załącznik C. Mapowanie licencji środowiska serwerowego - Załącznik D. Opis środowiska sieciowego LAN - Załącznik E. Zestawienie sprzętu sieciowego i oprogramowania - Załącznik F. Opis środowiska bazodanowego BD

Pojęcie	Definicja
	do niniejszego dokumentu.
Infrastruktura Zastana	Zastana Infrastruktura Informatyczna lub Zastana Infrastruktura Techniczna.
Zamawiający	Urząd Komunikacji Elektronicznej z siedzibą przy ul. Giełdowej 7/9, 01-211 Warszawa, nr NIP 527-23-67-496.
Wykonawca	Podmiot wyłoniony w ramach przetargu nieograniczonego przeprowadzonego na podstawie przepisów prawa zamówień publicznych do realizacji zadania/zadań zawartych w niniejszym dokumencie.
Centrum Przetwarzania Danych (CPD)	Lokalizacja, gdzie znajduje się infrastruktura odpowiedzialna za funkcjonowanie zasadniczego rozwiązania Systemu PLI CBD.
Centrala UAE	Lokalizacja Wydziału ds. PLI CBD w siedzibie Centrali UAE.
Komponent	Jest to składnik lub część Aplikacji PLI CBD, Infrastruktury Informatycznej PLI CBD. Przykłady Komponentów: moduł aplikacji, system operacyjny, serwer, przełącznik, dysk twardy, klawiatura, router itd.
Dokumentacja	Opis Systemu PLI CBD obejmujący wymagania oraz załączniki opisujące zastane Komponenty, jak również elementy dodane, wymienione lub uzupełnione w ramach realizacji niniejszej umowy jako efekt świadczonych usług.
Czas gotowości serwisowej	Stawienie się do dyspozycji Zamawiającego osób przeznaczonych do wykonywania usług. Dla Systemu PLI CBD jest to czas 7/24/365 (całą dobę przez cały tydzień w ciągu całego roku).
Proces biznesowy	Zasadnicze usługi: <ul style="list-style-type: none"> • lokalizacyjna E112 dla zgłoszeń ratunkowych, • przenośność numeru NP, • centralna baza numerów przeniesionych CBD, wykorzystywane przez Użytkowników Aplikacji PLI CBD.
Użytkownik	Podmiot korzystający z Aplikacji PLI CBD jako klient, korzystający z aplikacji SOU lub innego dedykowanego rozwiązania.
Użytkownik wewnętrzny	Personel obsługujący System PLI CBD.
Dni robocze	Oznacza każdy dzień od poniedziałku do piątku, z wyjątkiem dni ustawowo wolnych od pracy na terytorium Rzeczypospolitej Polskiej.
Roboczodzień	Ośmiogodzinny dzień pracy pracownika Wykonawcy dedykowanego do realizacji obsługi Systemu PLI CBD. 8 godzin zegarowych (8 x 60 minut) pracy jednej osoby.

3. Opis ogólny całego rozwiązania

Systemem PLI CBD zarządza Prezes UKE. W ramach UKE został utworzony Wydział do spraw PLI CBD, do którego zadań należy prowadzenie spraw związanych z organizacją i funkcjonowaniem Systemu PLI CBD. W ramach Wydziału funkcjonują dwa Centra Przetwarzania Danych (CPD): w Boruczy pod Warszawą oraz w Siemianowicach Śląskich, oraz komórka wsparcia w Centrali UKE.

Infrastruktura Techniczna wraz z Infrastrukturą Informatyczną Systemu Platformy Lokalizacyjno-Informacyjnej z Centralną Bazą Danych (PLI CBD) zbudowana została w dwóch Centrach Przetwarzania Danych oraz w Centrali Urzędu Komunikacji Elektronicznej. Lokalizacje CPD PLI CBD oraz Centrali UKE są następujące:

1. Centrum Przetwarzania Danych PLI CBD w Siemianowicach Śląskich, ul. Walerego Wróblewskiego 75 - współrzędne GPS (N 50,296355; E 19,006305).
2. Centrum Przetwarzania Danych PLI CBD w Boruczy gmina Strachówka - współrzędne GPS (N 52,342363; E 21,567950).
3. Centrala UKE - Warszawa, ul. Giełdowa 8/9 - współrzędne GPS (N 52,229793; E 20,977447).

System PLI CBD jest wynikiem pozytywnej realizacji dwóch projektów informatycznych. Pierwszy z projektów polegał na zbudowaniu centralnego Systemu PLI CBD zbierającego i udostępniającego informację o lokalizacji abonentów dzwoniących na numery alarmowe. Drugi projekt, opierając się na infrastrukturze technicznej i sprzętowej pierwszego, rozszerzył aplikacyjną funkcjonalność Systemu PLI CBD o obsługę wniosków związanych z przenoszeniem numerów oraz modułu wspierającego ten proces. Pierwsze komponenty Systemu PLI CBD: serwery, komputery stacjonarne, biblioteki taśmowe oraz większość infrastruktury technicznej zostały dostarczone przez wykonawcę w końcu 2010 roku. Większość sprzętu dostarczona była w 2011 roku, ale komponenty projektu PLI CBD2 dostarczane były na przełomie 2014 i 2015 roku (np. wykorzystywane w rozwiązaniu macierze dyskowe). Część sprzętu (m.in. serwery, load balancery) wdrożona była w roku 2021.

W dniu 26 czerwca 2015 roku dokonano odbioru końcowego Systemu PLI CBD2 i od tego momentu wykonawca Systemu najpierw PLI CBD, później PLI CBD2, przez okres dwóch lat świadczył usługi gwarancji, utrzymania (w tym wsparcia), jak również rozwoju, zaś usługi serwisu realizowane były z udziałem firm trzecich.

W dniu 27 grudnia 2017 roku podpisano umowę na usługi utrzymania, serwisu, gwarancji Systemu PLI CBD na okres 36 miesięcy. W ramach tej umowy Wykonawca dostarczył i dokonał wymiany części sprzętu serwerowego oraz sieciowego.

PLI CBD składa się z dwóch CPD w Boruczy i Siemianowicach Śląskich oraz wsparcia znajdującego się w Centrali UKE.

W każdym z CPD pracują Inspektorzy, którzy pracują w trybie ciągłym w 12-godzinnych zmianach, których zadaniem jest monitorowanie systemu PLI CBD.

Ponadto w Centrach Przetwarzania Danych PLI CBD pracują administratorzy od poniedziałku do piątku w trybie 12 godzinnym (07:30 -19:30):

- administrator baz danych,
- administrator aplikacji,
- administrator sieci,
- administrator serwerów.

Pracą CPD nadzorują Kierownicy zespołów, którzy pracują w tych obiektach.

W centrali UKE znajduje się Kierownictwo systemu PLI CBD, jak również zespół wsparcia pracujący od poniedziałku do piątku w trybie ruchomym 8 godzinnym (07:00 – 17:00).

Cały zespół PLI CBD składa się z:

- 12 inspektorów,
- 7 administratorów,
- 2 kierowników zespołów,
- 3 osób wsparcia,
- Naczelnika,
- Dyrektora.

Dostęp do CPD PLI CBD związany z realizacją umowy w zakresie usuwania awarii jest możliwy przez 24/7/365 po uprzednim zgłoszeniu. Dostęp w zakresie realizacji pozostałych zobowiązań wynikłych z postanowień umowy jest możliwy również w trybie 24/7/365 po uzgodnieniu z Kierownikiem Centrum Przetwarzania Danych. Dostęp do zasobów znajdujących się w Centrali UKE jest możliwy od poniedziałku do piątku w godzinach pracy Urzędu.

3.1 Środowisko aplikacyjne PLI CBD

Środowisko aplikacyjne PLI CBD zostało napisane w języku C# z wykorzystaniem technologii usług sieciowych (*web service*). Aplikacje wykorzystują bazy danych Microsoft SQL Server.

Dokładniejszy opis funkcjonalności Aplikacji PLI CBD, zawierający kompletną dokumentację, znajduje się na stronie UKE: <https://bip.uke.gov.pl/pli-cbd/>

Aplikacja PLI CBD ma następujące cztery funkcjonalności:

1. System pozyskiwania informacji o lokalizacji abonenta wzywającego pomocy i udostępnianie tych informacji do zainteresowanych służb - biznesowa usługa E112.

Dokładniejszy opis tej funkcjonalności znajduje się w plikach dokumentacji opisujących:

- wymagania dla interfejsu dla służb korzystających z Systemu PLI CBD (dokumentacja dostępna będzie do wglądu przez Wykonawcę w siedzibie Zamawiającego),
 - specyfikacje, sposób obsługi danych lokalizacyjnych, zasady współpracy z operatorami,
 - nowe formaty komunikatów E112.
2. System umożliwiający wymianę komunikatów pomiędzy dostawcami usług telekomunikacyjnych w procesach przenoszenia numerów telefonicznych przy zmianie dostawcy usług - biznesowa usługa NP.

Dokładniejszy opis tej funkcjonalności zawarty jest w plikach dokumentacji przedstawiających:

- opis procesów głównych przenoszenia numerów,
 - format i zawartość komunikatów Exx dla przenośności MNP,
 - format i zawartość komunikatów Exx dla przenośności FNP,
 - format i zawartość komunikatów numeracji udostępnionej,
 - instrukcję użytkownika - moduł zarządzania numeracją.
3. Centralna baza numeracji przydzielonej, numeracji udostępnionej oraz numerów przeniesionych.

Dokładniejszy opis tych funkcjonalności znajduje się w dokumentach zawierających:

- format i zawartość komunikatów numeracji udostępnionej,
 - instrukcję użytkownika - moduł zarządzania numeracją.
4. System Obsługi Użytkownika (SOU) - wsparcie użytkowników korzystających z Aplikacji PLI CBD.

Dokładniejszy opis tej funkcjonalności zawarty jest w plikach dokumentacji:

- instrukcja użytkownika - moduł SOU.

Właścicielem kodu źródłowego Standardowego Oprogramowania Aplikacyjnego Zastanej Aplikacji PLI CBD jest Zamawiający.

Kody źródłowe Standardowego Oprogramowania Aplikacyjnego wchodzącego w skład Zastanej Aplikacji PLI CBD zostaną przekazane Wykonawcy wyłonionemu w trakcie niniejszego przetargu po podpisaniu umowy. Na etapie przetargu będzie możliwy wgląd w kody Standardowego Oprogramowania Aplikacyjnego Zastanej Aplikacji PLI CBD bez możliwości wykonywania kopii.

3.2 Środowisko sprzętowe IT

Środowisko serwerowe Systemu PLI CBD w większości zbudowane zostało opierając się na serwerach firmy IBM z wykorzystaniem modeli x3650 generacji M4 oraz M5 (w zależności od daty instalacji) jak i serwery INSPUR NF5280M5. Szczegółowy spis sprzętu serwerowego znajduje się w *Załącznik A. Opis środowiska serwerowego SRV*. Jako oprogramowanie systemowe wykorzystano rodzinę produktów Microsoft Windows Server w wersji 2016.

Serwery, na których odbywa się przetwarzanie najistotniejszych danych z punktu widzenia Aplikacji PLI CBD (tj. serwery aplikacyjne, bazodanowe oraz kopii zapasowych (*backup*)), pracują bezpośrednio na maszynach fizycznych. Natomiast serwery pełniące rolę pomocniczych do obsługi środowiska Systemu PLI CBD (kontrolery domeny, urzędy certyfikacji, poczta elektroniczna, system antywirusowy, serwery testowe oraz serwery obsługujące system SOU) pracują na maszynach wirtualnych pod kontrolą systemu operacyjnego MS Windows 2016 z rolą Hyper-V. Poczta elektroniczna pracuje częściowo na maszynach fizycznych.

W obu CPD w Boruczy oraz Siemianowicach Śląskich została zainstalowana macierz dyskowa IBM Flash System 5200, która stanowi miejsce składowania plików głównych baz danych, plików maszyn wirtualnych itp. Macierz ta została zainstalowana w trakcie rozbudowy Systemu PLI CBD.

Jako zabezpieczenie przed utratą danych wykorzystywany jest system tworzenia kopii bezpieczeństwa BackupExec 21.4 firmy Symantec. System ten dla zapewnienia wysokiej niezawodności został wdrożony w środowisku klastrowym z dostępem do dwóch dwunapędowych bibliotek IBM TS 3200.

Ze względów bezpieczeństwa architektura Systemu PLI CBD została podzielona na kilka stref:

- strefa INET (strefa styku z siecią Internet)

W strefie INET umieszczone zostały serwery wymagające połączenia z zewnętrzną siecią Internet m.in.:

- serwer aktualizacji Microsoft WSUS - pobieranie aktualizacji Microsoft,
- Trellix – aktualizacja sygnatur antywirusowych z serwerów producenta,
- Trellix Security for Exchange – system antyspamowy uruchomiony na serwerach poczty

elektronicznej MS Exchange,

- Microsoft Exchange Edge – serwer brzegowy odpowiedzialny za wysyłanie / odbieranie wiadomości poczty elektronicznej,
- serwery bazodanowe i aplikacyjne SOU (System Obsługi Użytkowników) – dostęp dla operatorów / służb poprzez internet do aplikacji SOU. Serwery aplikacyjne SOU w każdym ośrodku zostały zduplikowane, a ruchem do każdej pary zarządza klaster urządzeń równoważenia obciążenia ruchu (*Load Balance*).

Środowisko w strefie INET zostało w całości zbudowane z wykorzystaniem zwirtualizowanych serwerów umieszczonych na trzech fizycznych serwerach działających pod obsługą środowiska Microsoft Hyper-V 2016.

Dodatkowo w strefie INET w Boruczy znajdują się także serwery środowiska testowego systemu SOU. Środowisko testowe systemu SOU w strefie INET również opiera się na wirtualizacji.

- Strefa DMZ (strefa styku z jednostkami podłączonymi do Aplikacji PLI CBD)

W każdym z ośrodków w strefie DMZ zostały umieszczone serwery aplikacyjne umożliwiające wymianę danych pomiędzy podłączonymi podmiotami (operatorzy i służby) a Systemem PLI CBD. Dodatkowo do strefy DMZ w Boruczy zostało włączone częściowo środowisko testowe. Serwery aplikacyjne w każdym ośrodku zostały zduplikowane, tak by uszkodzenie któregośkolwiek z nich nie degradowało ośrodka. Ruchem do każdej pary zarządza klaster urządzeń równoważenia obciążenia ruchu (*Load Balance*).

W strefie tej umieszczone zostały także stacje robocze personelu obsługującego System PLI CBD - 20 komputerów stacjonarnych ThinkCentre (M70eG41) i 19 komputerów przenośnych Lenovo ThinkPad Edge L540 (L54Q 20AU-S3G700).

- Strefa LAN (wewnętrzna strefa Systemu PLI CBD)

W strefie LAN umieszczone zostały serwery bazodanowe oraz serwery pomocnicze w tym: serwery aktualizacji, antywirusowy, kontrolery domeny, urzędy certyfikacji oraz serwer poczty elektronicznej. Część serwerów działa bezpośrednio na maszynach fizycznych (serwery bazy danych, serwery kopii zapasowych (*backup*) oraz serwer poczty elektronicznej), zaś pozostałe jako maszyny wirtualne pod kontrolą środowiska Microsoft Hyper-V.

W każdej lokalizacji z wykorzystaniem dwóch (2) fizycznych serwerów zbudowano redundantny klaster *failover* w środowisku wirtualizacji Hyper-V (Windows Server 2016 z rolą Hyper-V) z obsługą migracji on-line (*Live Migration*) dla wybranych maszyn wirtualnych.

Na serwerach ze środowiskiem Hyper-V uruchomiono maszyny wirtualne zapewniające następujące usługi:

- środowisko domenowe Active Directory,
- infrastruktura klucza publicznego (PKI),
- system antywirusowy Trellix,
- wewnętrzne serwery WSUS,
- system monitoringu,
- system Guardium,
- Kontrolery domeny DC (ang. *Domain Controller*)

Infrastruktura bazy Active Directory (AD) została zbudowana z podziałem na dwie (2) lokalizacje odpowiadające geograficznemu rozłożeniu kontrolerów domeny DC (CPD Borucza oraz CPD Siemianowice).

Domena AD składa się z 6 kontrolerów domeny z czego dwa (2) kontrolery są tylko do odczytu typu RODC (ang. *Read-Only DC*) i zapewniają autoryzację wewnętrznych użytkowników pracujących w Centrali UKE. Pracownicy w poszczególnych CPD łączą się do kontrolerów domen w swoich lokalizacjach lub awaryjnie w drugiej.

- Urząd certyfikacji (CA)

W Systemie PLI CBD została zbudowana dwupoziomowa Infrastruktura klucza publicznego (PKI) z jednym serwerem głównym typu *Root* oraz czterema (4) urzędami podrzędnymi (po dwa (2) w każdej lokalizacji) zapewniającymi certyfikaty na potrzeby funkcjonowania Systemu PLI CBD.

- Wewnętrzny serwer antywirusowy Trellix

System ochrony antywirusowej Trellix zapewnia ochronę dla wszystkich serwerów i stacji roboczych pracujących w środowisku Systemu PLI CBD. Ochronie podlegają wszystkie platformy systemowe z rodziny Windows. W sieci wewnętrznej w CPD PLI CBD w Siemianowicach Śląskich znajduje się wirtualny serwer z oprogramowaniem do zarządzania komputerami (*host*) i politykami e-Policy Orchestrator (ePO). W lokalizacji zapasowej w Borucza został wdrożony zapasowy serwer ePO pracujący w trybie agenta (*Agent Handler*). Serwer ePO wykorzystuje lokalny serwer bazodanowy Microsoft SQL 2014 w wersji Standard pracujący na klastrze Hyper-V dla zapewnienia ciągłości działania. Niedostępność serwera ePO nie stanowi żadnego problemu dla ciągłości działania ochrony antywirusowej AV (ang. *Anti-Virus*) serwerów oraz stacji roboczych.

- Wewnętrzny serwer WSUS

W każdej lokalizacji została zbudowana niezależna infrastruktura WSUS na potrzeby centralnej dystrybucji poprawek z wykorzystaniem dwóch (2) serwerów WSUS (wewnętrznego oraz zewnętrznego w strefie INET zapewniającego synchronizację z serwerami firmy Microsoft).

Wewnętrzny serwer WSUS zapewnia dystrybucję poprawek do wszystkich komputerów (*host*) będących członkami domeny, jak i komputerów (*host*) należących do grupy roboczej.

- Serwer monitoringu

W każdej lokalizacji znajduje się oddzielny system monitoringu obsługujący jedynie CPD, w którym się znajduje. System został zbudowany z wykorzystaniem dystrybucji Linux CentOS, na którym uruchomiono system monitoringu centreon oraz mrtg.

- Serwery poczty elektronicznej

Serwery poczty elektronicznej oparte na oprogramowaniu Microsoft Exchange 2019 pracują w trybie klastra DAG typu Active-Active. Każdy ośrodek posiada własną bazę skrzynek pocztowych, jednak w przypadku uszkodzenia bądź wyłączenia jednego z serwerów, drugi przejmuje jego funkcje, a użytkownik nie zauważa różnicy w działaniu.

W strefie INET każdego ośrodka znajdują się serwery brzegowe Exchange Edge odpowiedzialne za odbieranie / wysyłanie wiadomości poczty elektronicznej.

- Serwery kopii zapasowych (*backup*)

W każdej lokalizacji znajduje się niezależny klaster dwóch serwerów z oprogramowaniem do wykonywania kopii zapasowych (archiwizacji) Symantec Backup Exec 21.4. Klastery zostały zbudowane z wykorzystaniem roli Microsoft Failover Cluster w konfiguracji z dyskiem kworum (*quorum*).

Usługi objęte klastrem to: oprogramowanie Backup Exec 21.4, usługa FTP – wykorzystywana przez urządzenia sieciowe do odkładania konfiguracji, usługa serwera plików (File Server) – zawiera dyski domowe użytkowników wewnętrznych oraz współdzielony dysk sieciowy (usługa realizowana jest tylko na klastrze w CPD Siemianowice Śląskie i zapewnia dostęp dla użytkowników wewnętrznych we wszystkich lokalizacjach).

Kopie zapasowe zapisywane są na taśmach magnetycznych LTO 6 o pojemności 2.5 TB z wykorzystaniem czterech (po dwie w każdym CPD) bibliotek taśmowych IBM TS3200 z dwoma napędami każda.

- Macierze dyskowe

W obu lokalizacjach znajduje się sieć SAN zbudowana z wykorzystaniem protokołu Fibre Channel (FC) za pomocą dwóch (2) przełączników FC typ SAN24B-6 firmy IBM w każdej lokalizacji oraz macierzy dyskowej IBM wraz z dodatkową półką dyskową. Zdublowane przełączniki FC zapewniają ciągłość działania w przypadku awarii jednego z nich.

Na macierzach dyskowych zostały stworzone jednostki logiczne LU (ang. *Logic Unit*) pamięci masowej między innymi na potrzeby:

- baz danych,
- serwerów raportowych,
- maszyn wirtualnych,
- dysku kworum (*quorum*) dla klastrów: Hyper-V AD/PKI oraz serwerów kopii zapasowych (*backup*),
- dysków sieciowych użytkowanych przez użytkowników wewnętrznych.

Poszczególne komponenty aplikacyjne są zainstalowane na serwerach:

- aplikacja PLI CBD w zakresie usług E112 i NP jest zainstalowana na 12 serwerach aplikacyjnych, po 6 w każdej lokalizacji,
- aplikacja SOU jest zainstalowana na czterech (4) serwerach aplikacyjnych, po dwa (2) w każdej lokalizacji,
- aplikacja testowa w zakresie usług E112 i NP jest zainstalowana na jednym (1) serwerze aplikacyjnym w lokalizacji Borucza,
- aplikacja testowa SOU jest zainstalowana na jednym (1) serwerze aplikacyjnym w lokalizacji Borucza.

3.3 Opis Infrastruktury Technicznej

W celu poprawnego funkcjonowania Centrów Przetwarzania Danych PLI CBD (CPD PLI CBD) oraz zapewnienia najwyższego poziomu dostępności zabudowano szereg instalacji wchodzących w skład Infrastruktury Technicznej.

System klimatyzacji precyzyjnej utrzymuje parametry powietrza obiegowego w pomieszczeniach obsługiwanych - serwerowni i pomieszczeniu UPS (obsługa infrastruktury elektrycznej dla Systemu

PLI CBD). System zapewnia właściwą pracę urządzeń. W pomieszczeniach biurowo - administracyjnych zastosowano instalację klimatyzacji komfortu. Obiekty wyposażone są w centrale wentylacji służące do obróbki świeżego powietrza. Uzdatnione powietrze nawiewane jest do pokoi i pomieszczeń technicznych.

Dla spełnienia wymagań bezpieczeństwa przeprowadzono analizę zagrożeń oraz zdecydowano się na zaprojektowanie Elektronicznego Systemu Ochrony Obiektów. Rozwiązanie zapewnia monitoring techniczny placówek (SBMS) oraz bezpieczeństwo fizyczne (SCCTV, SKD oraz SSWiN).

W obiektach istnieją systemy sygnalizacji pożaru. Automatyczny system sygnalizacji pożarowej umożliwia wykrycie pożaru oraz sygnalizowanie i alarmowanie o pożarze w budynkach. Ochroną gaśniczą oraz detekcją pożaru została objęta serwerownia (komora typu *room-in-room*, przestrzeń właściwa oraz przestrzeń pod podłogą techniczną) oraz pomieszczenie UPS (przeźren właściwa oraz przestrzeń pod podłogą techniczną). Każde z chronionych pomieszczeń stanowi niezależną strefę gaśniczą. Centrale detekcji pożaru i sterowania gaszeniem oraz dwie baterie po dwie butle (w każdej lokalizacji są dwie ochraniane strefy, z których każda ma dwie butle z gazem, a jedna z tych stref w Boruczy ma dodatkową butlę inicjującą) ze środkiem gaśniczym zostały umieszczone poza chronionymi pomieszczeniami. System umożliwia również detekcję pożaru w pomieszczeniach obsługi. Sygnał pożaru kierowany jest do nadrzędnego systemu sygnalizacji pożaru.

Obecna Infrastruktura Techniczna PLI CBD składa się z następujących obszarów:

- szluz osobowa wraz z czytnikiem tęczówki oka,
- agregat prądowórczy,
- system zasilania gwarantowanego UPS,
- instalacje elektryczne, oświetleniowe, trasy kablowe, linie zasilające,
- system gaszenia pożaru gazem INERGEN, system wczesnej detekcji dymu VESDA,
- system telewizji przemysłowej CCTV,
- system kontroli dostępu SKD oraz system sygnalizacji włamania i napadu SSWiN,
- komora Lampertza oraz Sejf ogniotrwały Lampertza,
- system zarządzania budynkiem i monitoringu środowiska BMS,
- winda towarowa GEDA (Borucza),
- klimatyzacja precyzyjna,
- klimatyzacja komfortu,
- wentylacja mechaniczna,
- szafy RACK, jak i listwy zasilające.

4. Zasady współpracy Wykonawcy z Zamawiającym

4.1 Wdrożenie sprzętu i oprogramowania do Systemu PLI CBD

Wdrożenie sprzętu oraz oprogramowania leży po stronie Wykonawcy. Wdrożenie sprzętu oraz oprogramowania, jak również realizację pozostałych usług gwarancji, serwisu i utrzymania realizuje Wykonawca.

Tam gdzie będzie to konieczne Wykonawca zobowiązuje się dostarczyć sprzęt fabrycznie nowy wyprodukowany nie wcześniej niż 180 dni przed dniem dostawy, wolny od wad, kompletny i oryginalnie zapakowany. Sprzęt powinien pochodzić z oficjalnego kanału dystrybucji.

4.2 Zatrzymanie Systemu PLI CBD

W wypadku konieczności zatrzymania Systemu PLI CBD w czasie gotowości serwisowej, Zamawiający zostanie powiadomiony o tym fakcie z wyprzedzeniem co najmniej 5 (pięciu) dni roboczych. Sugestia czasowego zatrzymania Systemu PLI CBD lub któregoś z komponentów musi zostać poparta analizą i sprecyzowanymi przesłankami wskazującymi na taką konieczność. Musi to zostać udokumentowane, a zatrzymanie Systemu PLI CBD może nastąpić po zapoznaniu się z przedstawionymi analizami i zatwierdzeniu tej operacji przez Zamawiającego.

4.3 Zarządzanie zmianą

Wszelkie zmiany Systemu PLI CBD muszą być przeprowadzane zgodnie z obowiązującą u Zamawiającego procedurą zarządzania zmianą. Zarządzanie zmianą jest jednym z najważniejszych procesów, które muszą opierać się na sformalizowanych dokumentach począwszy od polityki zarządzania zmianą, poprzez procedury zarządzania zmianą, a na zaleceniach zmiany skończywszy.

Ważność tego procesu podkreśla fakt, iż część z dotychczas uruchomionych funkcjonalności biznesowych Systemu PLI CBD działa produkcyjnie i to w bardzo ostrych reżimach zarówno czasowych, wydajnościowych, jak i niezawodnościowych. Wykonawca w trakcie realizacji umowy zobowiązany będzie do dostosowania swoich prac instalacyjnych do panującego reżimu dotyczącego między innymi funkcji biznesowych realizowanych przez System PLI CBD, a związanego między innymi z koniecznością zapewnienia dostępu i pozyskania danych lokalizacyjnych w reżimie 24/7/365 dla usługi E112. W trakcie prac Wykonawca zobowiązany jest do przestrzegania procedury zarządzania zmianą obowiązującą u Zamawiającego dla Systemu PLI CBD.

5. Wymagania ogólne na usługi utrzymania

Identyfikator	U-WSP-001
Zamawiający wymaga stałego wsparcia oraz konsultacji zdalnych (poprzez telefon i pocztę elektroniczną e-mail) dotyczących:	
<ul style="list-style-type: none">• instalacji i konfiguracji środowiska Aplikacji PLI CBD oraz Infrastruktury Informatycznej,• zakresu funkcjonalnego Aplikacji PLI CBD oraz Infrastruktury Informatycznej,• zasad pracy z programami komputerowymi współpracującymi z Aplikacją PLI CBD oraz Infrastrukturą Informatyczną,• sytuacji awaryjnych związanych z Aplikacją PLI CBD oraz Infrastrukturą Informatyczną wchodzących w skład Systemu PLI CBD,• czas oczekiwania na udzielenie odpowiedzi przez Wykonawcę nie może przekroczyć dwóch dni roboczych. W przypadku potrzeby wykonania szczegółowej analizy Wykonawca powinien zwrotnie przekazać taką informację Zamawiającemu. W takich przypadkach czas oczekiwania na odpowiedź może być wydłużony przez Zamawiającego maksymalnie do 7 dni roboczych.	

Identyfikator	U-WSP-002
Zamawiający wymaga, by zdalna pomoc techniczna w przypadkach:	
<ul style="list-style-type: none">• problemów w eksploatacji Aplikacji PLI CBD oraz Infrastruktury Informatycznej wchodzących w skład Systemu PLI CBD,• Awarii/Błędów lub niesprawności Aplikacji PLI CBD oraz Infrastruktury Informatycznej.	
była realizowana za pośrednictwem programów (skryptów) narzędziowych, przesyłanych na nośnikach lub za pomocą łączności sieciowej zapewniającej zdalny dostęp autoryzowany jednorazowymi ustawieniami w celu:	
<ul style="list-style-type: none">• naprawiania i odtwarzania uszkodzonych danych,• zmian konfiguracji Aplikacji PLI CBD oraz Infrastruktury Informatycznej,	

- wykonania czynności pielęgnacyjnych,
- zabezpieczenia danych w związku z przebudową lub ponowną instalacją Aplikacji PLI CBD oraz Infrastruktury Informatycznej,
- konfigurowania i optymalizacji procesów replikacji,
- korekty w systemie synchronizacji czasu,
- korekty w systemie kopii zapasowych (*backup*).

Identyfikator	U-WSP-003
----------------------	------------------

W celu przywrócenia dostępności Systemu lub jego Komponentu Zamawiający dopuszcza możliwość dostępu zdalnego do Systemu PLI CBD na wcześniej uzgodnionych zasadach.

Identyfikator	U-WSP-004
----------------------	------------------

Wymaga się doraźnej pomocy w lokalizacjach Aplikacji PLI CBD oraz Infrastruktury Informatycznej w przypadkach trudności instalacyjnych lub awarii, co obejmuje następujące działania:

- analiza i adaptacja istniejącego środowiska Aplikacji PLI CBD oraz Infrastruktury Informatycznej,
- ustawienie parametrów Aplikacji PLI CBD oraz Infrastruktury Informatycznej,
- konfiguracja parametrów środowiska Aplikacji PLI CBD oraz Infrastruktury Informatycznej,
- instalacja oprogramowania środowisk Aplikacji PLI CBD oraz Infrastruktury Informatycznej,
- sprawdzenie konfiguracji środowisk Aplikacji PLI CBD oraz Infrastruktury Informatycznej,
- konfiguracja parametrów środowiska Aplikacji PLI CBD oraz Infrastruktury Informatycznej,
- testowanie poprawności działania Aplikacji PLI CBD oraz Infrastruktury Informatycznej,
- odtwarzanie środowiska Aplikacji PLI CBD z kopii zapasowych.

Identyfikator	U-WSP-005
----------------------	------------------

Strojenie i optymalizacja Aplikacji PLI CBD oraz Infrastruktury Informatycznej, wynikające z potrzeb:

- dostosowania do zmian konfiguracji sprzętowej i systemowej,
- bieżącej eksploatacji oraz na podstawie danych pochodzących z przeprowadzonego cyklicznie monitoringu Aplikacji PLI CBD oraz Infrastruktury Informatycznej, jest także obowiązkiem Wykonawcy.

Identyfikator	U-WSP-006
----------------------	------------------

Wykonawca w ramach utrzymania Systemu PLI CBD jest zobowiązany do utrzymywania w sposób automatyczny aktualności słowników danych przechowywanych w bazach Systemu PLI CBD. Wymagane jest okresowe, nie rzadziej niż raz w roku, weryfikowanie całościowe zgodności tych słowników z ich źródłem. Wykonawca zobowiązany będzie do przedstawienia Zamawiającemu raportu z realizacji tego zadania.

Identyfikator	U-WSP-007
----------------------	------------------

Wszystkie parametry Systemu PLI CBD (dostępność, niezawodność, czas skutecznej naprawy itp.) będą zestawiane w postaci miesięcznych raportów w celu oceny spełnienia wymagań w zakresie dostępności i niezawodności. Raporty będą również uwzględniać wszystkie prace wykonane przez Wykonawcę w danym okresie raportowym. Raporty będą przedstawiane do akceptacji Zamawiającego. Raport miesięczny będzie składany w terminie 10 dni kalendarzowych od dnia zakończenia danego miesiąca kalendarzowego.

Identyfikator	U-WSP-008
Wykonawca zobowiązany jest do wspomagania przedstawicieli Zamawiającego w konfigurowaniu Systemu PLI CBD związanego z dostosowaniem Systemu PLI CBD do bieżących zadań obsługowych Zamawiającego.	

Identyfikator	U-WSP-009
Niezawodność Systemu PLI CBD wynosi co najwyżej jedno (1) nieplanowane zatrzymanie na czas nie dłuższy niż 45 minut świadczenia którejkolwiek z dwóch usług (NP, E112) oferowanych przez System PLI CBD raz na trzy miesiące.	

Identyfikator	U-WSP-010
Wykonawca w ramach utrzymania Systemu PLI CBD jest zobowiązany do przeprowadzania cyklicznego (raz w roku trwania umowy) sprawdzania spójności zawartości baz danych oraz weryfikacji poprawności synchronizacji pomiędzy tymi bazami. W przypadku wykrycia niezgodności w danych lub błędnej synchronizacji, Wykonawca zobowiązany jest do przeprowadzenia akcji naprawczej, eliminującej wykryte błędy. Każdorazowo po przeprowadzeniu weryfikacji Wykonawca przedstawi raport wykrytych niezgodności, następnie po wykonaniu naprawy raport potwierdzający wyeliminowanie tych niezgodności.	

Identyfikator	U-WSP-011
Wszelkie zmiany Systemu PLI CBD muszą być przeprowadzane zgodnie z obowiązującą u Zamawiającego procedurą zarządzania zmianą. Wykonawca przed przystąpieniem do jakichkolwiek prac ingerujących w środowisko PLI CBD (rekonfiguracje, wdrożenia, aktualizacje itd.) zobowiązany jest na 14 dni przed planowanymi pracami przedstawić do akceptacji Zamawiającego wniosek o zmianę zgodny z szablonem obowiązującym u Zamawiającego. Powyższy termin może zostać skrócony jedynie w przypadku usuwania awarii.	

Identyfikator	U-WSP-012
Wszelkie zmiany na środowisku produkcyjnym powinny być poprzedzone testami na środowisku testowym Zamawiającego z minimum 7 dniowym wyprzedzeniem. Zmiany w środowisku produkcyjnym powinny być wykonywane w odstępie minimum 7 dniowym między lokalizacjami PLI CBD. Wyjątek stanowi sytuacja, w której ze względu na integralność aplikacji wymagane są zmiany w obu ośrodkach jednocześnie. Przykładowy schemat wykonywania prac: środowisko testowe → + min. 7 dni → Środowisko produkcyjne w lokalizacji Siemianowice → +min. 7 dni → Środowisko produkcyjne w lokalizacji Borucza. Powyższe terminy mogą zostać skrócone jedynie w przypadku usuwania awarii.	

Identyfikator	U-WSP-013
Wszelkie prace mające wpływ na działanie i dostępność serwerów świadczących usługi dla podmiotów zewnętrznych (w szczególności serwery aplikacyjne, serwery baz danych E112 oraz NP, serwery SOU aplikacyjne i ich serwery baz danych) muszą odbywać się w weekendowym nocnym oknie serwisowym. Weekendowe nocne okno serwisowe obejmuje następujące godziny: <ul style="list-style-type: none"> • piątek 22:00 – sobota 7:00, • sobota 22:00 – niedziela 7:00, • niedziela 22:00 – poniedziałek 7:00. 	

Niniejsze wymaganie ma zastosowanie w szczególności do wszelkiego rodzaju instalacji, aktualizacji i zmian konfiguracyjnych zarówno w zakresie oprogramowania systemowego, aplikacyjnego, jak również mikrokodów podzespołów tzw. firmware'ów.

Wymaganie to ma również zastosowanie w przypadku wymiany urządzeń na nowe.

Identyfikator	U-WSP-014
----------------------	------------------

Wykonawca przygotuje harmonogram realizacji Umowy na szablonie przekazanym przez Zamawiającego w formacie *.xlsx.	
---	--

6. Wymagania ogólne na usługi rozwoju

Identyfikator	R-WSP-001
----------------------	------------------

Wykonawca będzie dokumentować wprowadzane zmiany związane z rozwojem Systemu. Dokumentacja będzie przekazywana Zamawiającemu w cyklach związanych z wprowadzaniem tych zmian do Systemu.	
--	--

Identyfikator	R-WSP-002
----------------------	------------------

W przypadku gdy usługa polegać będzie na wprowadzeniu nowego elementu lub zastąpieniu dotychczasowego, to obowiązkiem Wykonawcy jest dokonać migracji wszystkich zasobów, aplikacji, usług, dostępu, ustawień monitorowania itd. z obecnego rozwiązania na nowo wprowadzone. Prace te w szczególności powinny obejmować:	
--	--

- zabezpieczenie wszelkich danych i konfiguracji z obecnych urządzeń,
- instalację fizyczną nowego urządzenia w szafie wraz z okablowaniem,
- instalację i konfigurację systemu. W razie konieczności zmiany wersji, Wykonawca wykona wszelkie czynności z tym związane, na docelowym urządzeniu,
- przeniesienie pełnej funkcjonalności i adaptacja do rozwiązania (instalacja i konfiguracja funkcji, reguł, skryptów, wyzwalaczy czasowych *crontab*) na nowe urządzenie z zachowaniem dotychczasowego nazewnictwa, adresacji itp.
- konfigurację systemu monitoringu, tak by zapewniał współpracę i poziom bezpieczeństwa przynajmniej taki jak zastępowane urządzenie,
- modyfikację konfiguracji systemu tworzenia kopii zapasowych, tak by obejmował nowe urządzenia zachowując dotychczasowe funkcjonalności oraz modyfikacje uzgodnione z Zamawiającym.

Identyfikator	R-WSP-003
----------------------	------------------

Wszelkie prace związane z migracją powinny być tak prowadzone, by nie miały wpływu na dostępność produkcyjnych funkcjonalności Systemu PLI CBD oraz usług biznesowych w żadnym z ośrodków. W razie braku takiej możliwości należy z wyprzedzeniem min. 14 dni kalendarzowych uzgodnić z Zamawiającym okna serwisowe i powiadomić podłączone podmioty o planowanej przerwie.	
---	--

Identyfikator	R-WSP-004
----------------------	------------------

Wykonawca zapewnia kompatybilność środowiska aplikacyjnego ze środowiskiem sprzętowym oraz środowiskiem oprogramowania standardowego zainstalowanym na środowisku sprzętowym. Kod źródłowy utrzymywanej Aplikacji PLI CBD musi dawać możliwość kompilacji w narzędziach kompilacyjnych.	
---	--

Identyfikator	R-WSP-005
Urządzenia powinny być fabrycznie nowe, posiadające wsparcie producenta urządzenia lub jego autoryzowanego przedstawiciela oraz mieć zapewniony dostęp do nowych wersji oprogramowania.	

Identyfikator	R-WSP-006
Wykonawca wykonując projekt konstrukcyjny rozwiązania powinien w pierwszej kolejności wykorzystać istniejące zasoby sprzętowe, programowe, infrastrukturalne, w drugiej zaś zasoby dodatkowe, które powinien zakupić, zamontować, skonfigurować uruchomić i wdrożyć. Nie przewiduje się powiększania powierzchni istniejących serwerowni w Centrach Przetwarzania Danych PLI CBD ani zwiększania zapotrzebowania na moc i klimatyzację. Urządzenia będą fabrycznie nowe, mające wsparcie producenta, nie znajdujące się w trybie „end of support” Wykonawca skonfiguruje nowe urządzenia zapewniając możliwie największą ich wydajność (np. stosując połączenia światłowodowe o przepustowości 10GbE, tam gdzie to możliwe zakupując wkładki SFP+ wraz z okablowaniem).	

Identyfikator	R-WSP-007
Jeżeli rozbudowa Systemu PLI CBD wymagać będzie doposażenia infrastruktury informatycznej i technicznej Wykonawca ma dostarczyć sprzęt, licencje oraz oprogramowanie niezbędne do jej uruchomienia.	

Identyfikator	R-WSP-008
Każde z nowych urządzeń należy podłączyć do systemu monitoringu.	

7. Wymagania w zakresie przetwarzania danych osobowych

Identyfikator	U-UODO-001
Podczas wszelkich prac prowadzonych w związku z realizacją przedmiotu umowy Wykonawca będzie uwzględniał ochronę danych osobowych w fazie projektowania oraz stosował domyślną ochronę danych osobowych (Art.25 RODO).	

Identyfikator	U-UODO-002
Wykonawca jeden (1) raz w ciągu trwania umowy dokona analizy ryzyka w związku z przetwarzaniem danych osobowych. Wyniki analizy zostaną przedstawione Zamawiającemu w formie opracowania.	

Identyfikator	U-UODO-003
Podczas wszelkich prac prowadzonych w związku z realizacją przedmiotu umowy Wykonawca będzie wdrażał odpowiednie środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa przetwarzanych danych osobowych (Art. 32 RODO).	

Identyfikator	U-UODO-004
W pierwszym kwartale trwania umowy Wykonawca dokona oceny skutków dla operacji przetwarzania danych osobowych. Podczas wszelkich prac prowadzonych w związku z realizacją przedmiotu umowy Wykonawca, przed wprowadzeniem zmian, w przypadku zmiany sposobu przetwarzania danych osobowych, dokona oceny skutków wprowadzanych zmian dla operacji przetwarzania danych osobowych (Art.35 RODO).	

8. Wymagania ogólne na usługi gwarancji

Identyfikator	G-WSP-001
Usługa gwarancji jest realizowana przez Wykonawcę przez okres 12 miesięcy od dnia podpisania umowy na wszystkie Komponenty wchodzące w skład: Aplikacji PLI CBD i Infrastruktury Informatycznej PLI CBD oraz na Komponenty dostarczone w okresie trwania Umowy.	

Identyfikator	G-WSP-002
Usługa gwarancji zapewnia Zamawiającemu w ramach umowy brak ponoszenia dodatkowych kosztów związanych z naprawą uszkodzenia komponentu Aplikacji PLI CBD i Infrastruktury Informatycznej PLI CBD, Umowa zawarta z Wykonawcą stanowi dokument gwarancyjny bez konieczności składania dodatkowego dokumentu na okoliczność udzielenia gwarancji.	

Identyfikator	G-WSP-003
Naprawa jest podstawową formą realizacji usługi gwarancji. Na czas naprawy Wykonawca zapewni stosowne obejście lub komponent zastępczy, tak by zachować reżim związany z niedostępnością usług biznesowych świadczonych przez Aplikację PLI CBD i przedstawionych w wymaganiu G-WSP-011 oraz G-WSP-012.	

Identyfikator	G-WSP-004
Proces obsługi naprawy gwarancyjnej komponentu obejmuje następujące działania:	
<ul style="list-style-type: none">• skuteczna naprawa zostanie wykonana w lokalizacji związanej z miejscem uszkodzenia,• czas skutecznej naprawy określony jest w wymaganiu G-WSP-011 oraz G-WSP-012.	

Identyfikator	G-WSP-005
W przypadku uzasadnionego braku możliwości naprawy komponentu w lokalizacji PLI CBD związanej z miejscem uszkodzenia, dopuszcza się naprawę w lokalizacji wybranej przez Wykonawcę.	
W przypadku naprawy urządzeń wyposażonych w nośniki informacji poza miejscem użytkowania, elementy tych urządzeń takie jak nośniki informacji pozostają wymontowane i składowane w CPD PLI CBD.	

Identyfikator	G-WSP-006
Komponenty, na których mogą być zapisane dane Zamawiającego (np. dyski) nie podlegają procesowi naprawy. W tym przypadku proces naprawy w usłudze gwarancji sprowadza się do dostarczenia i wdrożenia Komponentu o parametrach nie gorszych niż uszkodzony, realizującego identyczne funkcje i spełniającego identyczną rolę w strukturze Systemu PLI CBD. Dyski i nośniki, które są wymieniane lub zastępowane przez nowe, pozostają u Zamawiającego i nie podlegają zwrotowi do Wykonawcy.	

Identyfikator	G-WSP-007
W przypadku gdyby uszkodzenie Komponentu było na tyle duże, iż naprawa byłaby niemożliwa lub nieopłacalna ekonomicznie, Zamawiający dopuszcza dostarczenie w zamian Komponentu identycznego tego samego producenta lub sprzętu równoważnego o parametrach wydajnościowych nie gorszych niż	

uszkodzony, realizującego identyczne funkcje i spełniającego identyczną rolę w strukturze Systemu PLI CBD.

Identyfikator G-WSP-008

Zarządzanie usługą gwarancji leży po stronie Wykonawcy w ramach usługi utrzymania.

Identyfikator G-WSP-009

Wykonawca w trybie raz na miesiąc przedstawi Zamawiającemu raport ze świadczenia usług gwarancyjnych dla Systemu PLI CBD. Raport powinien zawierać zestawienie:

- uszkodzonych Komponentów Systemu PLI CBD wraz ze sposobem ich naprawy, wymiany i stemplami czasowymi rozpoczęcia i zakończenia naprawy,
- wszystkie parametry usługi (dostępność, niezawodność, czas skutecznej naprawy, czas obsługi zarządzania użytkownikami) będą rozliczane w miesięcznych okresach rozliczeniowych.

Identyfikator G-WSP-010

Po zakończeniu naprawy gwarancyjnej Wykonawca jest zobowiązany do przeprowadzenia instalacji Komponentu, uaktualnienia do stabilnej wersji oprogramowania, konfiguracji, optymalizacji i strojenia oraz integracji z Systemem PLI CBD, aby ten Komponent spełniał identyczne funkcje, jak i role, które były mu przypisane przed wystąpieniem awarii.

W przypadku wymiany Komponentu na nowy inny (w tym innego producenta) o parametrach nie gorszych niż Komponent uszkodzony, Wykonawca zapewni dostosowanie i integrację nowego Komponentu z wszelkimi systemami wchodzącymi w skład Systemu PLI CBD, które zapewniają nadzór, sterowanie i zarządzanie Komponentami. Zakres funkcji obsługi nowego Komponentu winien być co najmniej taki sam jak Komponentu podlegającego wymianie.

Identyfikator G-WSP-011

Przywrócenie dostępności Systemu PLI CBD lub jego Komponentu może nastąpić poprzez skuteczną naprawę lub zastosowanie obejścia na czas usuwania awarii. Zamawiający wymaga, by w ramach usługi utrzymania Wykonawca spełniał poniższe wymagania związane z czasem przywrócenia dostępności Systemu PLI CBD oraz czasem skutecznej naprawy Komponentu.

W poniższych wymaganiach dotyczących obsługi Błędów/Awarii czas przywrócenia dostępności wlicza się w czas skutecznej naprawy.

Typ Błędu/ Typ Awarii	Czas reakcji	Czas przywrócenia dostępności Systemu lub jego Komponentu	Czas skutecznej naprawy
Błąd/Awaria Krytyczny	≤ 0,25 godziny	2 godziny dla usługi lokalizacji zgłoszeń ratunkowych. 6 godzin dla usługi przeniesienia numeru	≤ 72 godziny
Błąd/Awaria Poważny	≤ 0,25 godziny	24 godzin	≤ 96 godziny
Błąd/Awaria	≤ 6 godziny	7 dni	≤ 30 dni
Błąd/Awaria Niskiej Kategorii	≤ 6 godziny	14 dni	≤ 30 dni

Powodem Błędu/Awarii może być uszkodzenie pojedynczego Komponentu lub kilku Komponentów wchodzących w skład Systemu PLI CBD. Może wystąpić również taka sytuacja, iż uszkodzenie pojedynczego Komponentu wpływa na nieprawidłowe działanie innych Komponentów.

Identyfikator		G-WSP-012	
Docelowa dostępność Systemu PLI CBD powinna być utrzymana na poziomie co najmniej 99,5 % w skali roku.			
Opis wymagania			
Miernik	Kategoria	Poziom świadczenia	
Czasy dostępności PLI CBD	Dostępność	7/24/365	
Maksymalna liczba awarii krytycznych	Niezawodność	≤ 1 na miesiąc	
Dopuszczalny okres utraty danych (RPO)	Ciągłość	0,5 godzin (dane aktualne)	

Identyfikator		G-WSP-013	
Zgłoszenia Błędu /Awarii mogą być dokonywane przez Zamawiającego:			
<ul style="list-style-type: none"> • pocztą elektroniczną: każdego dnia i przez całą dobę na adres poczty elektronicznej do upoważnionego przedstawiciela Wykonawcy, • telefonicznie: w czasie gotowości serwisowej na numer telefonu do upoważnionego przedstawiciela Wykonawcy, • poprzez automatyczne wysyłanie informacji o błędach przez system PLI CBD np. poprzez automatyczne maile. 			

Identyfikator		G-WSP-014	
Wykonawca zobowiązany jest dokonać potwierdzenia otrzymania zgłoszenia Błędu /Awarii w czasie nie dłuższym niż czas reakcji określony dla danej kategorii awarii (typ awarii), pocztą elektroniczną lub telefonicznie na numery telefonów obsługi Systemu PLI CBD.			

Identyfikator		G-WSP-015	
Liczba zgłoszeń Błędu /Awarii w ramach wynagrodzenia określonego w umowie jest nieograniczona.			

Identyfikator		G-WSP-016	
---------------	--	-----------	--

Wykonawca podejmie następujące działania po zgłoszeniu Błędu /Awarii:

- usunięcie Błędu /Awarii,
- usunięcie skutków Błędu /Awarii,
- sprawdzenie poprawności i skuteczności naprawy Systemu PLI CBD i Infrastruktury Informatycznej,
- sporządzenie planu działań zapobiegających powtórzeniu się tego samego Błędu /Awarii.

Usunięcie Błędu /Awarii oznacza dostarczenie sprawnych komponentów Systemu PLI CBD wolnych od wykrytej nieprawidłowości i przywrócenie sprawnego działania Systemu PLI CBD do stanu funkcjonalnego co najmniej takiego samego jak przed wystąpieniem Błędu /Awarii.

Identyfikator	G-WSP-017
----------------------	------------------

Usuwanie Błędu /Awarii musi być realizowane w trybie 24/7/365 (całą dobę, przez cały tydzień, w ciągu całego roku).

Identyfikator	G-WSP-018
----------------------	------------------

W przypadku konieczności zatrzymania Systemu PLI CBD Zamawiający zostanie powiadomiony o tym fakcie z wyprzedzeniem co najmniej 5 (pięciu) dni roboczych.

Identyfikator	G-WSP-019
----------------------	------------------

Wykonawca poinformuje Zamawiającego o postępach w usuwaniu Błędów/Awarii:

- dla Błędów/ Awarii Krytycznych oraz Poważnych nie rzadziej niż raz na 24 godziny,
- dla Błędów/ Awarii lub Błędów/ Awarii Niskiej Kategorii nie rzadziej niż raz na pięć (5) dni.

9. Wymagania ogólne na usługi wdrożeniowe

Identyfikator	U-WDR-001
----------------------	------------------

W ramach wdrożenia Wykonawca w szczególności:

1. Wykona analizę przedwdrożeńową.
2. Dostarczy standardowe oprogramowanie systemowe oraz standardowe oprogramowanie aplikacyjne oraz dokona ich koniecznej parametryzacji, konfiguracji lub innych zmian w celu spełnienia wymagań Umowy i zapewnienia poprawnego działania Systemu.
3. Zainstaluje oprogramowanie na infrastrukturze Zamawiającego.
4. Przetestuje i uruchomi wdrażane komponenty.
5. Przeprowadzi warsztaty dla wybranej grupy pracowników Zamawiającego.
6. Udzieli gwarancji na przeprowadzone prace.
7. Przeprowadzi wdrożenie zgodnie z obowiązującą procedurą zarządzania zmianą.
8. Dostarczy niezbędne licencje.
9. Przedstawi i uzgodni z Zamawiającym harmonogram prac wdrożeniowych.
10. Przedstawi i uzupełni dokumentację powykonawczą.

Identyfikator	U-WDR-002
----------------------	------------------

Zamawiający ma prawo do weryfikacji należytego wykonania usług wdrożeniowych dowolną metodą, w tym także z wykorzystaniem opinii zewnętrznego audytora. W szczególności uzgodnienie określonych scenariuszy testowych nie wyklucza prawa do weryfikacji prac innymi testami.

10. Wymagania pozafunkcjonalne

Bezpieczeństwo

Identyfikator	X-FUN-001
System PLI CBD musi spełniać co najmniej wymagania bezpieczeństwa określone w: <ul style="list-style-type: none">• Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781)• Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2020 r. poz. 346)• Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2020 r. poz. 344)• Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz. U. z 2019 r. poz. 2134 z późn. zm.)• Rozporządzeniu Rady Ministrów z dnia 28 grudnia 2015 r. w sprawie organizacji i funkcjonowania systemu gromadzącego i udostępniającego informacje i dane od przedsiębiorcy telekomunikacyjnego(Dz. U. 2015 poz. 2333).• Rozporządzeniu Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. 2011 nr 159 poz. 948).• Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2017 r. poz. 2247), i zdefiniowanych wymaganiach OPZ.	
Identyfikator	X-FUN-002
Przydzielanie uprawnień i uwierzytelnianie użytkowników wewnętrznych musi być oparte na bazie Active Directory.	
Identyfikator	X-FUN-003
Wszelkie operacje osób użytkujących System PLI CBD związane z dodanymi lub zmodyfikowanymi funkcjonalnościami muszą być rejestrowane w plikach typu <i>log</i> .	
Identyfikator	X-FUN-004
Wszelkie próby nieautoryzowanego dostępu powinny być rejestrowane w plikach typu <i>log</i> , a informacja o takich próbach mających charakter prób włamania się do Systemu PLI CBD lub nadużycia powinna trafiać do obsługi Systemu PLI CBD.	
Identyfikator	X-FUN-005
Wszystkie dane cyfrowe pozyskiwane z zewnętrznych źródeł powinny podlegać weryfikacji i kontroli poprzez dedykowany system antywirusowy lub inne rozwiązanie alternatywne.	
Identyfikator	X-FUN-006

Wymaga się, żeby zarówno cały System PLI CBD, jak i jego poszczególne części składowe charakteryzowały się wysokim poziomem bezpieczeństwa. Bezpieczeństwo obejmuje odporność na ataki oraz wykrywanie ataków zewnętrznych i wewnętrznych. System PLI CBD i wchodzące w jego skład dostarczone przez Wykonawcę oprogramowanie umożliwi instalowanie poprawek podnoszących bezpieczeństwo Systemu PLI CBD.

Identyfikator	X-FUN-007
----------------------	------------------

Komunikacja pomiędzy Systemem PLI CBD i podmiotami zewnętrznymi korzystającymi z danych gromadzonych w Systemie PLI CBD będzie odbywać się m.in. poprzez powszechnie dostępną sieć Internet. Wymaga się, żeby cała komunikacja z Systemem PLI CBD prowadzona poprzez Internet była szyfrowana i chroniona za pomocą metod kryptograficznych. Wymagane jest, aby Wykonawca zapewnił mechanizmy zabezpieczeń i autoryzacji dostępu do Systemu PLI CBD zgodne z już wbudowanymi mechanizmami.

Identyfikator	X-FUN-008
----------------------	------------------

Aplikacja PLI CBD musi zapewniać możliwość definiowania przez administratorów zestawu uprawnień dla poszczególnych ról w Aplikacji PLI CBD.

Identyfikator	X-FUN-009
----------------------	------------------

Aplikacja PLI CBD musi spełniać wymagania określone w ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 poz. 1000 z późn. zm). oraz rozporządzeniach wykonawczych do tej ustawy.

Ponadto musi to być zgodne z:

- Dyrektywą Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłająca decyzję ramową Rady 2008/977/WSiSW,
- Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Identyfikator	X-FUN-010
----------------------	------------------

System PLI CBD musi posiadać zabezpieczenie przed niekontrolowanym obciążeniem wywołanym wskutek nadmiernego ruchu generowanego przez integrowane systemy zewnętrzne.

Neutralność technologiczna

Identyfikator	X-FUN-011
----------------------	------------------

Na każdym etapie w Systemie PLI CBD powinny być przestrzegane zasady neutralności technologicznej tak, aby docelowe rozwiązanie było systemem otwartym, który wykorzystuje otwarte standardy, opublikowane przez uznane organizacje standaryzacyjne. Specyfikacja wykorzystanych protokołów komunikacyjnych, interfejsów i formatów danych powinna być publicznie dostępna.

Identyfikator	X-FUN-012
----------------------	------------------

Definicje interfejsów, protokołów i formatów danych muszą być opracowane w taki sposób, by dowolny podmiot zewnętrzny był w stanie stworzyć własne komponenty komunikujące się z Systemem PLI CBD, z zachowaniem wymogów bezpieczeństwa.

Identyfikator	X-FUN-013
Wszystkie zewnętrzne interfejsy Systemu PLI CBD muszą wykorzystywać standardowe (a co najmniej otwarte) formaty danych i protokoły, przez co rozumie się:	
<ul style="list-style-type: none">• w obszarach stosowalności standardów wymienionych w Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2017 r. 2247) stosowane są te standardy,• w obszarach nie objętych tym Rozporządzeniem, dla których istnieją powszechnie akceptowane otwarte standardy, stosowane są te standardy,• w obszarach, gdzie nie ma powszechnie akceptowanych otwartych standardów:<ul style="list-style-type: none">○ stosowane są komercyjne <i>de facto</i> standardy (powszechnie stosowane specyfikacje) pod warunkiem, że ich właściciele udostępniają publicznie specyfikacje niezbędne dla wdrożenia standardu i nie nakładają żadnych ograniczeń ani nie pobierają opłat za ich wykorzystanie i eksploatację, lub○ stosowane są specyfikacje specyficzne (własne) spełniające warunek określony powyżej, rozszerzony również o brak ograniczeń i opłat dotyczących modyfikacji i rozszerzania tych specyfikacji.	

Identyfikator	X-FUN-014
W żadnym wypadku nie mogą być stosowane specyfikacje, które stanowią tajemnice (nie zostały i nie mogą być podane do publicznej wiadomości) lub których wykorzystanie oraz implementacja podlega ograniczeniom lub opłatom związanym z prawami autorskimi lub pokrewnymi.	

Identyfikator	X-FUN-015
Aby standard można było uznać za otwarty, musi on spełniać następujące warunki:	
<ul style="list-style-type: none">• standard jest zatwierdzony i jest utrzymywany przez organizację nie nastawioną na zysk (<i>non-profit</i>), a jego ciągły rozwój odbywa się na zasadzie procedury podejmowania decyzji w otwartym gronie zainteresowanych uczestników (przez porozumienie lub głosowanie itp.),• standard jest opublikowany, a dokument go specyfikujący jest dostępny nieodpłatnie lub za symboliczną opłatą. Jego kopiowanie, dystrybucja i stosowanie (w całości, w części lub w zmodyfikowanej postaci) powinno być dozwolone dla wszystkich zainteresowanych – bez opłaty albo za opłatą symboliczną,• prawa autorskie, w tym ewentualne zawarte w standardzie patenty, zostały w nieodwołalny sposób udostępnione jako wolne od opłat licencyjnych.	

Przeność

Identyfikator	X-FUN-016
System PLI CBD musi cechować się przenośnością, rozumianą jako możliwość jego adaptacji do zmieniających się rozwiązań sprzętowych i programowych. Podstawowymi metodami osiągnięcia przenośności są:	
<ul style="list-style-type: none">• zastosowanie szeroko dostępnych i znanych języków oprogramowania i środowisk (platform) wspieranych na wielu platformach sprzętowo-systemowych,	

- brak ograniczeń licencyjnych w zakresie wykorzystywania oprogramowania standardowego i dedykowanego na innych niż dostarczone przez Wykonawcę platformach sprzętowo-systemowych przy zachowaniu ograniczeń na liczbę komputerów i procesorów, na których wykonywane jest oprogramowanie,
- konstrukcja modułowa Systemu PLI CBD, umożliwiająca wymianę poszczególnych modułów na nowe moduły zgodne pod względem interfejsów z dotychczasowymi, z zachowaniem pełnej funkcjonalności Systemu PLI CBD,
- dokładne udokumentowanie protokołów współpracy poszczególnych modułów,
- zastosowanie otwartych standardów.

W szczególności Wykonawca zobowiązany jest do udokumentowania:

- struktury Systemu PLI CBD (podział na moduły),
- zakresu i formatu danych przechowywanych w poszczególnych elementach składowych Systemu PLI CBD (moduły, aplikacje standardowe, aplikacje dedykowane),
- interfejsów wymiany danych:
 - pomiędzy elementami składowymi Systemu PLI CBD,
 - pomiędzy Systemem PLI CBD a otoczeniem.

Elastyczność

Identyfikator	X-FUN-017
System PLI CBD musi cechować się dużą elastycznością, rozumianą jako możliwość dostosowania Systemu PLI CBD do zmieniających się wymagań funkcjonalnych wynikających ze zmieniającego się stanu prawnego oraz zmian związanych z wydajnością bezpieczeństwa i komunikacją z systemami zewnętrznymi.	

Identyfikator	X-FUN-018
W szczególności elastyczność Systemu PLI CBD powinna być rozumiana także jako możliwość rozbudowy Systemu i rozszerzania jego zakresu funkcjonalnego.	

Identyfikator	X-FUN-019
Niezbędne jest zachowanie szerokich możliwości konfiguracji Systemu PLI CBD za pomocą plików konfiguracyjnych i parametrów w taki sposób, aby zapewnić możliwość utrzymania technicznej i merytorycznej żywotności Systemu PLI CBD przez długi okres eksploatacji przy jednoczesnej minimalizacji liczby koniecznych modyfikacji kodów źródłowych.	

Użyteczność

Identyfikator	X-FUN-020
Aplikacja PLI CBD powinna być wyposażona w jednolity, graficzny interfejs użytkownika, zaprojektowany zgodnie z zasadami ergonomii.	

Identyfikator	X-FUN-021
Interfejs użytkownika końcowego musi być polskojęzyczny. Zamawiający oczekuje również polskiego interfejsu użytkownika w odniesieniu do modułów administracyjnych.	

Identyfikator	X-FUN-022
----------------------	------------------

Klientem Aplikacji PLI CBD powinna być przeglądarka internetowa. Aplikacja powinna działać identycznie dla przynajmniej pięciu (5) przeglądarek (Internet Explorer, Microsoft Edge, Firefox, Opera i Chrome) w aktualnych wersjach oraz w co najmniej dwóch poprzednich.

Identyfikator	X-FUN-023
----------------------	------------------

Aplikacja PLI CBD musi umożliwiać automatyczne skalowanie interfejsu zgodnie z rozdzielczością ekranu.	
--	--

Identyfikator	X-FUN-024
----------------------	------------------

Aplikacja PLI CBD powinna wyświetlać użytkownikowi komunikaty informujące o błędach.	
--	--

Identyfikator	X-FUN-025
----------------------	------------------

Aplikacja PLI CBD musi działać w środowiskach systemów operacyjnych dla serwerów wykorzystując technologię 64-bitową. Dostęp do Aplikacji PLI CBD winien być przez przeglądarkę pracującą w środowisku systemu operacyjnego 32- i 64-bitowego.	
--	--

Efektywność energetyczna

Identyfikator	X-FUN-026
----------------------	------------------

Proponując rozwój Systemy PLI CBD Wykonawca zapewni efektywność energetyczną wyrażoną w poborze energii elektrycznej przez wdrażane Komponenty zgodnie z kryteriami określonymi w programie Energy Star uwzględniając rankingi SPEC.	
--	--

Dokumentacja

Identyfikator	X-FUN-027
----------------------	------------------

Dokumentacja Systemu PLI CBD zostanie zaktualizowana albo rozszerzona przez Wykonawcę o dokumentację powykonawczą w związku z wykonanymi pracami. Dokumentacja zostanie zaktualizowana przez Wykonawcę, także na wyraźną prośbę Zamawiającego.	
---	--

Współpraca między Wykonawcą a podmiotami

Identyfikator	X-FUN-027
----------------------	------------------

Wykonawca zobligowany jest do współpracy z wykonawcami innych podsystemów/funkcjonalności, które wchodzi, bądź będą wchodziły w skład Systemu PLI CBD. Wykonawcy ci na zlecenie Zamawiającego mogą prowadzić prace w dowolnej lokalizacji PLI CBD, które mogą wpływać na System PLI CBD. Na poziomie umowy z tymi wykonawcami Zamawiający zobliguje ich do współpracy z Wykonawcą.	
--	--

Ograniczenia i zależności projektowe i realizacyjne

Identyfikator	X-FUN-028
----------------------	------------------

Wykonanie modyfikacji oraz dodanie nowych funkcjonalności nie może mieć negatywnego wpływu na funkcjonujący System PLI CBD.	
---	--

Identyfikator	X-FUN-029
----------------------	------------------

Nie dopuszcza się możliwości przerwy w świadczeniu którejkolwiek z usług, oferowanych przez System PLI CBD dla klientów zewnętrznych jak również dla klientów wewnętrznych. W związku z tym niedopuszczalne jest jednoczesne wyłączenie dwóch CPD PLI CBD w tym samym czasie. Wszelkie prace planowane powinny być tak realizowane by zachować to wymaganie. Dotyczy to również prac związanych z rozbudową i modernizacją CPD, dla których w przypadku konieczności przerwania świadczenia usług obowiązuje utrzymanie dostępności usług 99,5% w skali roku.

Identyfikator	X-FUN-030
----------------------	------------------

Wykonawca jest zobligowany do przygotowania procedury wycofania zmiany ze środowiska produkcyjnego w przypadku negatywnego wyniku testów powdrożeniowych. Zamawiający może podjąć niezależnie decyzję o wycofaniu zmiany przez Wykonawcę, jeżeli po wdrożeniu zaobserwowany zostanie spadek wydajności pracy Aplikacji PLI CBD lub wystąpią inne błędy w funkcjonowaniu Aplikacji PLI CBD lub Infrastruktury Informatycznej.

Identyfikator	X-FUN-031
----------------------	------------------

W sytuacji, gdy działania Wykonawcy, związane z wycofaniem zmiany na żądanie Zamawiającego, nie przyniosą rezultatu Wykonawca zobowiązuje się do zapewnienia na swój koszt i ryzyko przywrócić w terminie 24 godzin funkcjonalność i wydajność Aplikacji PLI CBD sprzed wprowadzonej zmiany.

Identyfikator	X-FUN-032
----------------------	------------------

Zasady komunikacji na linii Zamawiający – Wykonawca zostaną ustalone po podpisaniu umowy. W ramach ustaleń zostaną określone telefony kontaktowe, formularze kontaktowe, adres e-mail służący do zgłaszania awarii, dane osób odpowiedzialnych za realizację usług po stronie zarówno Zamawiającego jak i Wykonawcy etc. Określone zasady komunikacji i dane kontaktowe zostaną spisane na protokole potwierdzającym te ustalenia. Ich zmiana w trakcie trwania umowy też potwierdzana będzie protokołem.

Wydajność

Identyfikator	X-FUN-033
----------------------	------------------

Wszelkie zmiany w zakresie Aplikacji PLI CBD oraz Infrastruktury Informatycznej nie mogą pogorszyć wydajności obsługi wywołań alarmowych oraz obsługi procesów przenoszenia numerów które wynoszą:

- do 15 tys. wywołań alarmowych w ciągu 1 minuty,
- do 40 mln wywołań alarmowych w ciągu miesiąca,
- do 200 tys. procesów przeniesienia numerów w ciągu jednej doby,
- do 4,5 mln. procesów przeniesienia numerów w ciągu miesiąca.

11. Wymagania na utrzymanie środowiska serwerowego SRV

Identyfikator	U-SRV-001
----------------------	------------------

Wykonawca co najmniej raz (1) w roku przeprowadzi serwis wszystkich serwerów, macierzy dyskowych, bibliotek w ramach Infrastruktury Informatycznej w lokalizacjach PLI CBD obejmujący:

- przegląd zawartości plików zdarzeń *log* urządzeń wraz z ewentualnym usunięciem przyczyn rejestrowanych problemów (m.in. serwery, macierze, biblioteki, IMM, WebGUI),
- wykonanie niezbędnych aktualizacji urządzeń (m.in. BIOS, IMM, sterownik RAID, oprogramowanie systemowe *firmware* urządzeń),
- czyszczenie napędów bibliotek taśmowych.

Z prewencyjnego serwisu serwerów, macierzy dyskowych, bibliotek w ramach Infrastruktury Informatycznej w lokalizacjach Systemu PLI CBD, Wykonawca opracuje zbiorczy raport i przekaże go Zamawiającemu.

Identyfikator	U-SRV-002
---------------	-----------

Wykonawca co najmniej raz (1) w roku przeprowadzi w obu lokalizacjach PLI CBD testy pełnego odtworzenia z kopii zapasowych przynajmniej dwóch (2) serwerów z środowiska produkcyjnego z grupy obsługujących aplikacje E112, NP lub SOU oraz odpowiednie dla nich serwery bazodanowe w każdej z lokalizacji. Test obejmuje:

- przygotowanie środowiska do testu odtworzeniowego,
- odtworzenie systemu operacyjnego serwerów z kopii zapasowej dostępnej w bazie kopii,
- odtworzenie wymaganych baz danych,
- porównanie stanu serwera źródłowego ze stanem serwera odtworzonego,
- ocena możliwości osiągnięcia przez serwer odtworzony pełnego stanu (100%) serwera źródłowego,
- przygotowanie scenariuszy testowych weryfikujących poprawność działania aplikacji E112, NP., SOU na odtwarzanych serwerach,
- wykonanie testów (z przygotowanych scenariuszy), potwierdzających poprawność działania aplikacji na odtwarzanych serwerach.

Odtworzenie nie może pochodzić z kopii wykonanej wyłącznie do celu testu.

Przed przystąpieniem do testów Wykonawca:

- przygotowuje plan powrotu gwarantujący pełną funkcjonalność Systemu PLI CBD sprzed testu,
- przygotowuje dokładny scenariusz odtworzenia (wraz z listami kontrolnymi (*checklist*) pozwalającymi na weryfikację poprawności odtworzenia dla każdego serwera) wybranych systemów z kopii zapasowej.

Po przeprowadzonych testach Wykonawca przekaże Zamawiającemu stworzone przez siebie procedury odtworzenia wszystkich systemów działających w PLI CBD (całego PLI CBD) w formie „krok po kroku”, zawierające dokładne informacje o samym odtworzeniu systemu z kopii zapasowej, jak i wszystkich kolejnych krokach wymaganych do pełnego odtworzenia danego systemu (jak np. dodatkowe ręczne synchronizacje itp.).

W razie wykrycia nieprawidłowości w funkcjonowaniu systemu kopii zapasowych (w tym harmonogramu, retencji danych), Wykonawca po konsultacji z Zamawiającym, wdroży wszelkie modyfikacje konfiguracji systemu zapewniające poprawne tworzenie kopii.

Identyfikator	U-SRV-003
<p>Wykonawca co najmniej dwa (2) razy do roku przeprowadzi przegląd środowiska serwerowego Infrastruktury Informatycznej PLI CBD oraz stacji roboczych obejmujący:</p> <ul style="list-style-type: none"> • przegląd zawartości plików zdarzeń <i>log</i> na wszystkich systemach operacyjnych wraz z ich analizą i rozwiązaniem problemów zidentyfikowanych na bazie plików <i>log</i> (m.in. pliki zdarzeń <i>log</i> samego systemu operacyjnego wraz z plikami zdarzeń <i>log</i> dla zainstalowanych ról oraz pliki zdarzeń <i>log</i> dla oprogramowania zainstalowanego na serwerze np. BackupExec, Trellix,...), • przegląd konfiguracji zasad grup (GPO). Weryfikacja obecnej konfiguracji pod kątem dobrych praktyk oraz 'harderingu' systemów operacyjnych. Po wykonanym przeglądzie proponowane zmiany zostaną wdrożone w porozumieniu z Zamawiającym, • monitoring: <ul style="list-style-type: none"> ○ zajętości zasobów dyskowych, ○ wykorzystania CPU, ○ wykorzystania pamięci RAM. • sprawdzenie synchronizacji czasu, • wykonanie testów bezpieczeństwa w celu wykrycia podatności bezpieczeństwa wraz z usunięciem wykrytych podatności na wszystkich serwerach, co zostanie potwierdzone ponownymi testami środowiska, • wykonane testy, usunięcie luk oraz ponowne testy, Wykonawca udokumentuje w przekazanej Zamawiającemu dokumentacji. Przekazana dokumentacja zawierać będzie m.in. szczegółowy opis (instrukcję) usuwania wykrytych podatności, • instalację wymaganych poprawek bezpieczeństwa i aktualizacji krytycznych oprogramowania, a następnie aktualizację obrazów w repozytorium Desktop Central OSDeployer (uwzględniając wdrażane poprawki), • aktualizację oprogramowania do najnowszych stabilnych wersji. W przypadku wygaśnięcia wsparcia od producenta oprogramowania, Wykonawca zakupi i wdroży aktualizację do wersji aktualnie wspieranej. Wykonawca dokona aktualizacji oprogramowania na co najmniej 6 miesięcy przed planowaną datą wygaśnięcia wsparcia producenta oprogramowania. <p>Pomiędzy kolejnymi przeglądami należy zachować odstęp min. 5 miesięcy, nie więcej jednak niż 7 miesięcy. Pierwszy przegląd należy przeprowadzić do 3 miesięcy po podpisaniu umowy.</p>	

Identyfikator	U-SRV-004
<p>Wykonawca co najmniej raz (1) do roku przeprowadzi przegląd środowiska archiwizacji danych, obejmujący:</p> <ul style="list-style-type: none"> • przegląd zawartości plików zdarzeń <i>log</i> na wszystkich komponentach wchodzących w skład środowiska tworzenia kopii zapasowych (w szczególności bibliotekach, serwerach oraz oprogramowaniu) wraz z ich analizą i rozwiązaniem zidentyfikowanych problemów, • przegląd zadań tworzenia kopii zapasowych wraz z ewentualną ich rekonfiguracją, • instalację najnowszych uaktualnień (Feature Pack) wszystkich komponentów oprogramowania archiwizującego wykorzystywanego przez Zamawiającego. <p>W przypadku wygaśnięcia wsparcia od producenta oprogramowania, Wykonawca zakupi odpowiednią ilość licencji i wdroży aktualizację do wersji aktualnie wspieranej. Wykonawca dokona aktualizacji oprogramowania na co najmniej 6 miesięcy przed planowaną datą wygaśnięcia wsparcia producenta oprogramowania.</p>	

Identyfikator	U-SRV-005
<p>Wykonawca co najmniej raz (1) do roku przeprowadzi przegląd licencji dla wszystkich systemów serwerowych, obejmujący:</p> <ul style="list-style-type: none"> • przegląd i weryfikację ilości i poprawności wykorzystania licencji wszystkich serwerowych systemów operacyjnych, • przegląd i weryfikację ilości i poprawności wykorzystania licencji dla wszystkich aplikacji i serwisów działających na wszystkich serwerach (w szczególności: Guardium, Exchange, SQL, BackupExec, Trellix, IIS, i innych). <p>W przypadku ujawnienia braku jakichkolwiek licencji Wykonawca dokona ich zakupu i instalacji niezależnie od czasu w jakim powstał niedobór licencji (aktualne na dzień sporządzenia SIWZ mapowanie licencji i ich przypisanie oraz konfiguracje sprzętowe zostały załączone do dokumentacji przetargowej w formie załączników).</p> <p>W przypadku wygaśnięcia wsparcia od producenta oprogramowania, Wykonawca zakupi odpowiednią ilość licencji i wdroży aktualizację do wersji aktualnie wspieranej. Po wdrożonej aktualizacji żaden z elementów Systemu PLI CBD nie może ulec pogorszeniu ze względu na szybkość i niezawodność działania. Jeżeli utrzymanie dotychczasowych parametrów wydajnościowych będzie wiązało się z koniecznością doposażenia lub wymiany sprzętu, Wykonawca dokona stosownych zakupów i je wdroży. Ostatni przegląd oprogramowania serwerowego w ramach zawartej umowy, powinien wykazać, iż wsparcie producenta oprogramowania, w ciągu sześciu (6) miesięcy od zakończenia obowiązywania umowy nie wygaśnie dla żadnego oprogramowania. Jeżeli do sześciu (6) miesięcy od daty zakończenia umowy miałyby wygasnąć wsparcie producenta jakiegokolwiek oprogramowania, Wykonawca zakupi i wdroży odpowiednią aktualizację przed zakończeniem czasu trwania umowy z zastrzeżeniem identycznych warunków jak dla zakończenia wsparcia w czasie obowiązywania umowy.</p> <p>Wynikiem prac ma być raport z przeglądu licencji, którego częścią będą m.in.:</p> <ul style="list-style-type: none"> • potwierdzenie poprawności licencjonowania środowiska PLI CBD przez niezależny od Wykonawcy Podmiot zewnętrzny posiadający niezbędne kompetencje w tym zakresie, • zestawienie / Mapowanie licencji - tj. szczegółowy wykaz licencji z przypisaniem do każdego serwera Systemu PLI CBD. 	

Identyfikator	U-SRV-006
<p>Wykonawca wykupi u producentów sprzętu i oprogramowania wsparcie (lub zapewni wsparcie na poziomie nie odbiegającym od wsparcia producenta) dla wszystkich urządzeń wskazanych w załączniku B „Zestawienie sprzętu serwerowego i oprogramowania” oraz całego sprzętu i oprogramowania dostarczonego lub wdrożonego w ramach realizacji Umowy.</p> <p>Powyższe wsparcie musi zostać zakupione/udzielone minimum na okres jaki dany sprzęt będzie użytkowany w trakcie trwania Umowy, tj:</p> <ul style="list-style-type: none"> • dla sprzętu i oprogramowania, które nie są przewidziane do wymiany - na cały okres trwania Umowy, • dla sprzętu i oprogramowania wymienianego - do czasu jego wymiany, • dla sprzętu i oprogramowania nowego (aktualizowanego i wdrażanego) – od momentu wdrożenia do końca Umowy. 	

Identyfikator	U-SRV-007
<p>Wykonawca wykupi dla macierzy oraz przełączników SAN (wymieniowych w załączniku B Zestawienie sprzętu serwerowego i oprogramowania) wsparcie u producenta sprzętu minimum na czas trwania Umowy.</p> <p>Zamawiający dopuszcza wymianę macierzy i przełączników SAN na nowe tego samego producenta o parametrach nie gorszych niż obecnie zainstalowane rozwiązanie. Wykonawca przed dostarczeniem nowego systemu SAN musi przedstawić do akceptacji Zamawiającego analizę porównawczą parametrów oferowanego systemu SAN do obecnie zainstalowanego w PLI CBD.</p> <p>Zamawiający zastrzega sobie prawo do odrzucenia zaproponowanego rozwiązania w przypadku ujawnienia gorszych parametrów w nowym rozwiązaniu względem obecnego.</p>	

Identyfikator	U-SRV-008
<p>Przynajmniej dwa (2) razy do roku Wykonawca przeprowadzi przegląd systemu antywirusowego, obejmujący minimum:</p> <ul style="list-style-type: none"> • przegląd logów oprogramowania, • przegląd konfiguracji i weryfikację jej pod kątem dobrych praktyk jak i obecnych zagrożeń, • Weryfikację poprawnej komunikacji wszystkich końcówek klienckich z serwerem zarządzającym, • weryfikację aktualności oprogramowania i aktualizację do najnowszej stabilnej wersji, • usunięcie wykrytych nieprawidłowości (po konsultacji z Zamawiającym). • testy poprawności działania modułu antyspamowego (Trellix - MSME), zainstalowanego na serwerach Exchange Edge <p>Po przeprowadzonym przeglądzie Wykonawca prześle Zamawiającemu raport zawierający m.in.:</p> <ul style="list-style-type: none"> • wykryte nieprawidłowości, • wykaz zmian wprowadzonych w celu usunięcia wykrytych nieprawidłowości, • Rekomendacje zmian w systemie antywirusowym, mające na celu podniesienie bezpieczeństwa całego systemu PLI CBD. <p>Pomiędzy kolejnymi przeglądami należy zachować odstęp min. 5 miesięcy, nie więcej jednak niż 7 miesięcy. Pierwszy przegląd należy przeprowadzić do 3 miesięcy po podpisaniu umowy.</p>	

Identyfikator	U-SRV-009
<p>Wykonawca wykupi dla bibliotek (wymieniowych w załączniku B Zestawienie sprzętu serwerowego i oprogramowania) wsparcie u producenta sprzętu minimum na czas trwania Umowy.</p> <p>Zamawiający dopuszcza wymianę bibliotek na nowe tego samego producenta o parametrach nie gorszych niż obecnie zainstalowane rozwiązanie. Wykonawca przed dostarczeniem nowych bibliotek musi przedstawić do akceptacji Zamawiającego analizę porównawczą parametrów oferowanego sprzętu do obecnie zainstalowanego w PLI CBD.</p> <p>Zaproponowane rozwiązanie musi gwarantować przynajmniej identyczną z obecną przepustowość wykonywania kopii. Ponadto nowe rozwiązanie musi oferować możliwość instalacji tej samej ilości taśm co w obecnym rozwiązaniu, a same taśmy powinny gwarantować zapis przynajmniej takiej samej ilości danych co obecnie wykorzystywane.</p> <p>W przypadku wymiany bibliotek Wykonawca dostarczy odpowiednie do nich taśmy, o pojemności jednostkowej nie mniejszej niż obecne, w ilości 150% pojemności taśmowej wszystkich bibliotek (w tym przypadku wymaganie R-SRV-009 traci ważność).</p>	

Zamawiający zastrzega sobie prawo do odrzucenia zaproponowanego rozwiązania w przypadku ujawnienia gorszych parametrów w nowym rozwiązaniu względem obecnego.

12. Wymagania na rozwój środowiska serwerowego SRV

Identyfikator	R-SRV-001
<p>Wykonawca dostarczy i wdroży dwa (2) serwery w miejsce obecnych (S-LAN-SRVHV1345, B-LAN-SRVHV2345). Wymagania ogólne dotyczące migracji zasobów na nowe serwery zostały opisane w R-SRV-005.</p> <p>Dostarczone serwery muszą spełniać minimalne wymagania opisane poniżej:</p> <ul style="list-style-type: none">• Obudowa Rack 19" o wysokości max. 2U z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.• Płyta główna z możliwością zainstalowania min. dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym oraz posiadać chipset dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.• Serwer musi pozwalać na analizę sprzętu (minimum dysków, pamięci) i powiadomienie o możliwości wystąpienia awarii (tak zwana analiza Predictive Failure Analysis)• Zainstalowane dwa procesory min. 12-rdzeniowe, min. 2.1GHz, klasy x86 dedykowane do pracy z zaferowanym serwerem umożliwiające osiągnięcie wyniku min. 37000 na podstawie PerformanceTest w teście CPU Mark według wyników Average CPU Mark w konfiguracji dwu procesorowej opublikowanych na stronie http://www.cpubenchmark.net/.• Minimum 256GB DDR4 RDIMM 3200MT/s, , należy zainstalować 16 kości pamięci 16 GB RAM, po 8 sztuk na procesor. Płyta główna powinna obsługiwać do 1TB pamięci RAM. Dodatkowo pamięć musi obsługiwać następujące funkcjonalności Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing• Minimum trzy sloty PCIe generacji 4• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)• Dodatkowe karty:<ul style="list-style-type: none">○ 1x dwuportowa karta 1GbE Ethernet w standardzie BaseT• Zainstalowane 6 dysków SSD SAS o pojemności min. 960GB, 2,5" Hot-Plug, 12 Gbit/s, 2,5" (RAID 0 / RAID 1: 2 dyski, RAID 5: 3 dyski, 1 zapasowy).• Sprzętowy kontroler dyskowy RAID, posiadający min. 4GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących.• 4 x USB z czego nie mniej niż 1x USB 3.0• 2xVGA z czego jeden na panelu przednim• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200• Redundantne zasilacze Hot-Plug, o mocy pozwalającej na poprawną pracę serwera przy jednym zasilaczu.• Moduł TPM 2.0• Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.• Karta zdalnego zarządzania: niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:	

- zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
- zdalne monitorowanie i informowanie o statusie serwera;
- szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika;
- możliwość podmontowania zdalnych wirtualnych napędów;
- wirtualną konsolę z dostępem do myszy, klawiatury;
- wsparcie dla IPv6;
- wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH;
- integracja z Active Directory;
- możliwość obsługi przez dwóch administratorów jednocześnie;
- wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.

Wykonawca dostarczy jeden (1) serwer do lokalizacji CPD PLI CBD w miejscowości Borucza oraz jeden (1) serwer do lokalizacji CPD PLI CBD w miejscowości Siemianowice Śl.

Identyfikator	R-SRV-002
---------------	-----------

Wykonawca dostarczy i wdroży dwa (2) serwery w miejsce obecnych (S-LAN-SRVRDS1231, B-LAN-SRVRDS2231). Wymagania ogólne dotyczące migracji zasobów na nowe serwery zostały opisane w R-SRV-005.

Dostarczone serwery muszą spełniać minimalne wymagania opisane poniżej:

- Obudowa Rack 19" o wysokości max. 2U z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.
- Płyta główna z możliwością zainstalowania min. dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym oraz posiadać chipset dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
- Serwer musi pozwalać na analizę sprzętu (minimum dysków, pamięci) i powiadomienie o możliwości wystąpienia awarii (tak zwana analiza Predictive Failure Analysis)
- Zainstalowane dwa procesory min. 12-rdzeniowe, min. 2.1GHz, klasy x86 dedykowane do pracy z zaferowanym serwerem umożliwiające osiągnięcie wyniku min. 37000 na podstawie PerformanceTest w teście CPU Mark według wyników Average CPU Mark w konfiguracji dwu procesorowej opublikowanych na stronie <http://www.cpubenchmark.net/>.
- Minimum 256GB DDR4 RDIMM 3200MT/s, , należy zainstalować 16 kości pamięci 16 GB RAM, po 8 sztuk na procesor. Płyta główna powinna obsługiwać do 1TB pamięci RAM. Dodatkowo pamięć musi obsługiwać następujące funkcjonalności Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing
- Minimum trzy sloty PCIe generacji 4
- Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
- Dodatkowe karty:
 - 1x dwuportowa karta 1GbE Ethernet w standardzie BaseT
- Zainstalowane 6 dysków SSD SAS o pojemności min. 960GB, 2,5" Hot-Plug, 12 Gbit/s, 2,5" (RAID 0 / RAID 1: 2 dyski, RAID 5: 3 dyski, 1 zapasowy).
- Sprzętowy kontroler dyskowy RAID, posiadający min. 4GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących.
- 4 x USB z czego nie mniej niż 1x USB 3.0

- 2xVGA z czego jeden na panelu przednim
- Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
- Redundantne zasilacze Hot-Plug, o mocy pozwalającej na poprawną pracę serwera przy jednym zasilaczu.
- Moduł TPM 2.0
- Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
- Karta zdalnego zarządzania: niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:
 - zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
 - zdalne monitorowanie i informowanie o statusie serwera;
 - szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika;
 - możliwość podmontowania zdalnych wirtualnych napędów;
 - wirtualną konsolę z dostępem do myszy, klawiatury;
 - wsparcie dla IPv6;
 - wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH;
 - integracja z Active Directory;
 - możliwość obsługi przez dwóch administratorów jednocześnie;
 - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.

Wykonawca dostarczy jeden (1) serwer do lokalizacji CPD PLI CBD w miejscowości Borucza oraz jeden (1) serwer do lokalizacji CPD PLI CBD w miejscowości Siemianowice Śl.

Identyfikator	R-SRV-003
<p>Wszystkie serwery dostarczone w ramach wymagań od R-SRV-001 do R-SRV-002 muszą ponadto spełniać poniższe wymagania wspólne:</p> <ul style="list-style-type: none"> • Dostarczone serwery muszą pochodzić od tego samego producenta • Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022. • Posiadać dokumentację w języku polskim lub angielskim. • Producent musi oferować możliwość zdalnego (telefonicznie lub przez stronę internetową) sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego. • 7 lat gwarancji i wsparcia producenta • Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. • Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. 	

- Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

Identyfikator	R-SRV-004
Wykonawca wdroży serwery dostarczone w ramach wymagań R-SRV-001 do R-SRV-002 w środowisku Zamawiającego oraz dokona migracji danych na nowe serwery.	
W ramach migracji należy wykonać m. in. :	
<ul style="list-style-type: none"> • Kopie zapasowe systemu operacyjnego, oprogramowania i danych na serwerach. • Zamontowanie serwerów w szafach RACK w miejsce obecnych. • Konfigurację kart zdalnego zarządzania. • Podłączenie serwerów do przełącznika KVM. • Instalację systemu operacyjnego oraz oprogramowania wraz z migracją danych ze starych serwerów. • Rekonfigurację pozostałych elementów systemu jeśli to konieczne (np. przełączniki FC z uwagi na nowe karty FC). • Cały proces powinien być przeprowadzony z możliwie najmniejszą niedostępnością świadczonych usług oraz jeśli to konieczne w wyznaczonym oknie serwisowym. • Migracja funkcji i usług z wycofywanych serwerów na nowe. • Rekonfiguracja systemu monitoringu polegająca na odłączeniu starych i podłączeniu nowych serwerów do systemu monitorowania. • Rekonfiguracja systemu tworzenia kopii zapasowych uwzględniająca wprowadzone zmiany. • Rekonfiguracja systemu antywirusowego uwzględniająca wprowadzone zmiany. 	
Wykonawca dokupi ewentualne brakujące licencje Windows Server w wersji bieżącej wspieranej, tak by zgodnie z zasadami licencjonowania możliwa była praca systemu operacyjnego na wszystkich zainstalowanych procesorach i rdzeniach.	

Identyfikator	R-SRV-005
Wykonawca zakupi i wdroży w środowisku testowym Zamawiającego licencje Microsoft RDS CAL pozwalające na jednoczesną pracę minimum 4 użytkowników na każdym z serwerów:	
<ul style="list-style-type: none"> • domena testowa – 9 serwerów • serwery typu standalone – 6 serwerów 	

Identyfikator	R-SRV-006
Wykonawca dostarczy 18 szt. komputerów przenośnych spełniających poniższe wymagania minimalne:	
<ul style="list-style-type: none"> • Obudowa komputera charakteryzująca się podwyższoną odpornością na uszkodzenia mechaniczne oraz przystosowana do pracy w trudnych warunkach termicznych - oferowany model notebooka musi spełniać normy MIL-STD-810H. Jednoznaczne informacje na temat powyższej certyfikacji MIL-STD 810H muszą znajdować się w ogólnodostępnej dokumentacji technicznej producenta komputera • Matryca: <ul style="list-style-type: none"> ○ matryca TFT 15-16" z podświetleniem w technologii LED; 	

- rozdzielczość minimum FHD 1920x1080;
- technologia IPS;
- jasność minimum 250 cd/m²;
- kąt otwarcia pokrywy ekranu min.180 stopni;
- ekran matowy;
- obudowa mechanizmu otwierania matrycy (zawiasów) w całości wykonana ze stopów metali celem pełnego zabezpieczenia wrażliwych elementów na uszkodzenia mechaniczne;
- Płyta główna
 - zaprojektowana i wyprodukowana przez producenta oferowanego komputera lub na jego zlecenie,
 - trwale oznaczona (na laminacie płyty głównej) na etapie produkcji nazwą producenta oferowanej jednostki i dedykowana dla danego modelu urządzenia,
 - wyposażona w BIOS producenta komputera, zawierający numer seryjny komputera oraz numer seryjny płyty głównej.
- Procesor
 - wielordzeniowy ze zintegrowaną kartą graficzną, zaprojektowany do pracy w komputerach przenośnych, klasy x86, minimum 10 rdzeni, osiągający minimum 13500 punktów na podstawie PerformanceTest w teście CPU Mark według wyników Average CPU Mark opublikowanych na <http://www.cpubenchmark.net/>.
- Pamięć RAM
 - Minimum 16 GB 3200 MHz non-ECC, DDR4;
 - Minimum 2 sloty na pamięć RAM, w tym 1 wolny;
 - Możliwość rozbudowy pamięci do min. 64GB
- Dysk twardy
 - dysk o pojemności min. 1 TB SSD PCIe NVMe Gen.4
- Interfejsy
 - Wbudowana karta sieciowa WLAN pracująca w standardzie ax
 - zintegrowany port RJ-45 (nie dopuszcza się adapterów, kart zewnętrznych, itp)
 - Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition;
 - Trwale wbudowane w obudowie komputera głośniki Dolby Audio , porty słuchawek i mikrofonu (typu COMBO), wbudowane dwa mikrofony, zintegrowana technologia Dolby Voice;
 - Fabrycznie zintegrowana w obudowie matrycy kamera video FHD, hybrydowa z funkcją IR (obsługa Windows Hello) oraz z mechaniczną zasłoną obiektywu
 - Sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszenia głośników oraz mikrofonu (mute);
 - HDMI 2.0 b
 - minimum 1x Thunderbolt 4;
 - minimum 1x USB-C 3.2;
 - minimum 2x USB-A 3.2 (Gen. 1),
 - Bluetooth 5.1;
 - wbudowany touchpad

-
- Bateria
 - Minimum 57Wh;
 - Komputer dostarczony z fabryczną ładowarką USB-C/ Thunderbolt min. 65W;
 - Dedykowana dioda pozwalająca na optyczną weryfikację stanu ładowania baterii komputera przy zamkniętej matrycy;
 - -System szybkiego ładowania baterii – minimum 80% w ciągu 60 minut;
- Waga typowa według dokumentacji producenta komputera – maksimum 1,8kg;
- Preinstalowany system operacyjny Microsoft Windows 10 Pro 64 bit, dostarczona licencja Microsoft Windows 11 Pro OEM;
- oferowany model komputera w oferowanej konfiguracji bez stacji dokującej musi obsługiwać minimum 2 ekrany zewnętrzne o rozdzielczości minimalnej 3840x2160 każdy,
- Klawiatura odporna na zalanie cieczą (potwierdzone w ogólnodostępnej dokumentacji producenta komputera), układ US, wyposażona w klawiaturę numeryczną;
- Zintegrowany dTPM 2.0 (dedykowany układ sprzętowy bezpośrednio na płycie głównej, niezintegrowany z chipsetem płyty głównej)
- parametry potwierdzone w ogólnodostępnej dokumentacji producenta komputera;

Wykonawca dostarczy i wdroży cztery (4) komputery do lokalizacji CPD PLI CBD w miejscowości Borucza, siedem (7) komputerów do lokalizacji CPD PLI CBD w miejscowości Siemianowice Śl. oraz siedem (7) komputerów do lokalizacji PLI CBD w Warszawie.

Wdrożenie obejmować będzie m.in.:

- instalacje komputera na stanowisku w danej lokalizacji,
- dodanie komputera do domeny Active Directory,
- instalację agentów systemu antywirusowego oraz Desktop Central.

Przygotowanie obrazu wzorcowego komputerów na potrzeby instalacji nienadzorowanej przez system Desktop Central OSDeployer.

Identyfikator	R-SRV-007
<p>Wykonawca dostarczy 4 szt. komputerów stacjonarnych spełniających poniższe wymagania minimalne:</p> <ul style="list-style-type: none"> ● Obudowa <ul style="list-style-type: none"> ○ Typu TOWER ○ Zaprojektowana i wyprodukowana przez producenta komputera, trwale oznaczona nazwą producenta komputera (na etapie produkcji). ○ ● Płyta główna <ul style="list-style-type: none"> ○ Z chipsetem rekomendowanym przez producenta procesora ○ Z obsługą TPM 2.0 ○ Zawierająca min. następujące gniazda: <ul style="list-style-type: none"> - 1 x PCI Express 3.0 x16, - 1 x PCI Express 3.0 x1, - M.2 obsługujący dyski PCIe. ● Procesor <ul style="list-style-type: none"> ○ wielordzeniowy zaprojektowany do pracy w komputerach stacjonarnych lub stacjach roboczych, klasy x86, o wydajności minimum 25000 punktów na podstawie 	

PerformanceTest w teście CPU Mark według wyników Average CPU Mark opublikowanych na <http://www.cpubenchmark.net/>.

- Pamięć RAM
 - Min. 16 GB DDR4
 - Minimum 4 sloty pamięci RAM, w tym 2 wolne
 - Możliwość rozbudowy do min. 64 GB
- Dysk twardy
 - Min. 1 TB SSD M.2 PCIe
- Karta graficzna oferująca możliwość podpięcia 2 ekranów zewnętrznych o rozdzielczości minimalnej 3840x2160 każdy
- Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition.
- Interfejsy
 - Karta sieciowa 100/1000 – złącze RJ45 z obsługą WoL
 - Minimum 6 x USB w tym: minimum 3x USB3.2 z przodu obudowy (jeden z portów w standardzie USB-C) i minimum 3 x USB z tyłu obudowy;
 - porty słuchawek i mikrofonu na przednim lub tylnym panelu,
 - port wyjścia dźwięku z tyłu komputera
 - Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.

- Klawiatura przewodowa w układzie US lub EU,
- Mysz przewodowa (scroll),
- Przewód zasilający o długości min. 1,8m
- Zasilacz o zakresie napięcia wejściowego 100-240V
- System operacyjny Windows 11 PRO lub równoważny.

Wykonawca dostarczy oraz wdroży dwa (2) komputery do lokalizacji CPD PLI CBD w miejscowości Borucz, oraz dwa (2) komputery do lokalizacji CPD PLI CBD w miejscowości Siemianowice Śl.

Wdrożenie obejmować będzie m.in.:

- Instalację komputera na stanowisku w danej lokalizacji
- Dodanie komputera do domeny Active Directory
- Instalację agentów systemu antywirusowego oraz Desktop Central
- Przygotowanie obrazu wzorcowego komputerów na potrzeby instalacji nienadzorowanej przez system Desktop Central OSDeployer

Identyfikator	R-SRV-008
---------------	-----------

Wykonawca wdroży w systemie pocztowym Zamawiającego mechanizmy:

- SPF (Sender Policy Framework),
- DKIM (DomainKeys Identified Mail),
- DMARC (Domain-based Message Authentication Reporting and Conformance).

W ramach prac Wykonawca:

- w pierwszej kolejności przeprowadzi z Administratorami Zamawiającego szkolenie dot. sposobu działania i możliwych konfiguracji wdrażanych mechanizmów,

- przygotuje i przedstawi do akceptacji Zamawiającemu szczegółowy plan prac zapewniający wdrożenie rozwiązania w sposób minimalizujący przerwy w działaniu systemu pocztowego Zamawiającego,
- przeprowadzi testy mające na celu potwierdzenie poprawności działania wdrożonego rozwiązania,
- będzie monitorował system pocztowy Zamawiającego przez pierwsze 30 dni od wdrożenia, a na podstawie zebranych danych oceni wpływ wdrożenia na przepływ poczty / ilość odrzucanych wiadomości,
- przedstawi raport końcowy zawierający m.in. szczegóły dotyczące konfiguracji poszczególnych mechanizmów, rezultat przeprowadzonych testów oraz monitoringu.

Identyfikator	R-SRV-009
Wykonawca dostarczy 120 szt. taśm LTO6 o pojemności 2,5 TB wraz z kompletem etykiet (barcode labels – opis zostanie uzgodnionym z Zamawiającym).	
Wykonawca dostarczy sześćdziesiąt (60) taśm do lokalizacji CPD PLI CBD w miejscowości Borucza, oraz sześćdziesiąt (60) taśm do lokalizacji CPD PLI CBD w miejscowości Siemianowice Śl.	

13. Wymagania na utrzymanie środowiska sieciowego LAN

Identyfikator	U-LAN-001
Wykonawca co najmniej raz (1) w roku przeprowadzi prewencyjny przegląd wszystkich urządzeń sieciowych w CPD PLI CBD obejmujący:	
<ul style="list-style-type: none"> • Przegląd plików zdarzeń log urządzeń wraz z ich analizą i usunięciem przyczyn rejestrowanych problemów. • Aktualizacje oprogramowania (do najnowszych, stabilnych wersji) sprzętu sieciowego posiadanego przez Zamawiającego i wykorzystywanego w PLI CBD (zgodnie z załącznikiem E. Zestawienie sprzętu sieciowego i oprogramowania). • Przeprowadzenie analizy wykorzystania zasobów teletransmisyjnych sieci i urządzeń sieciowych, która będzie zakończona raportem oraz wdrożeniem niezbędnych modyfikacji. • Odkurzenie wnętrza sprzętu, w tym oczyszczenie wentylatorów. 	
Z prewencyjnego przeglądu wszystkich urządzeń sieciowych w ramach Infrastruktury Informatycznej w lokalizacjach PLI CBD, Wykonawca opracuje zbiorczy raport i przekaże go Zamawiającemu.	

Identyfikator	U-LAN-002
Wykonawca co najmniej raz (1) w roku przeprowadzi testy mające na celu kontrolę redundancji urządzeń oraz poprawnego działania systemu monitoringu. Odłączone od sieci LAN oraz sieci energetycznej zostanie każde urządzenie z pary, tak aby sprawdzić działanie trybu pracy: aktywny/oczekujący (active/standby) lub aktywny/aktywny (active/active).	

Identyfikator	U-LAN-003
----------------------	------------------

Wykonawca co najmniej raz (1) do roku przeprowadzi skanowanie sieci wyszukujące możliwe podatności oraz luki w zabezpieczeniach. Skanowanie zostanie przeprowadzone z sieci Internet oraz z wewnątrz sieci w ośrodkach CPD PLI CBD w Siemianowicach Śląskich, Boruczy i Warszawie Centrala UAE. W przypadku wykrytych podatności Wykonawca je usunie, oraz przeprowadzi ponowny test weryfikujący poprawność usunięcia luki. Wykonane testy, usunięcie luk oraz ponowne testy, Wykonawca udokumentuje w przekazanej Zamawiającemu dokumentacji.

Identyfikator	U-LAN-004
----------------------	------------------

Wykonawca dostarczy niezbędne licencje (Partner Support Renewal, PAN-DB URL Filtering, Threat Prevention) dla dwóch (2) urządzeń firewall Palo Alto 3020. Wykonawca dokona instalacji oraz konfiguracji licencji. Zainstalowane licencje muszą być ważne co najmniej do czasu wymiany na nowe urządzenia (zgodnie z wymaganiem R-LAN-001).

Identyfikator	U-LAN-005
----------------------	------------------

Wykonawca zakupi przedłużenie do końca okresu trwania umowy supportu producenta dla czterech urządzeń Juniper SRX SRX550-645AP-M.

Identyfikator	U-LAN-006
----------------------	------------------

Wykonawca zakupi przedłużenie do końca okresu trwania umowy supportu producenta dla czterech (4) urządzeń Juniper SRX 4100.

Identyfikator	U-LAN-007
----------------------	------------------

Wykonawca zakupi przedłużenie do końca okresu trwania umowy supportu producenta dla czterech (4) urządzeń IAP-305-RW spełniających role bezprzewodowych punktów dostępowych w Centrali UAE Warszawa

Identyfikator	U-LAN-008
----------------------	------------------

Wykonawca zakupi przedłużenie do końca okresu trwania umowy supportu producenta, oraz nowej licencji S-JSPLT-S1-P dla dwóch (2) platform zarządzania sieciami JunoSpace. W przypadku gdy producent nie oferuje supportu do końca okresu trwania umowy, Wykonawca wykupi przedłużenie supportu producenta na okres maksymalnie dostępny, a w pozostałym czasie obowiązywania umowy Wykonawca zapewni support we własnym zakresie.

Identyfikator	U-LAN-009
----------------------	------------------

Wykonawca zakupi przedłużenie do końca okresu trwania umowy supportu producenta dla czterech (4) urządzeń PSA3000. W przypadku gdy producent nie oferuje supportu do końca okresu trwania umowy, Wykonawca wykupi przedłużenie supportu producenta na okres maksymalnie dostępny, a w pozostałym czasie obowiązywania umowy Wykonawca zapewni support we własnym zakresie.

Identyfikator	U-LAN-010
----------------------	------------------

Wykonawca zakupi przedłużenie do końca okresu trwania umowy supportu producenta dla czterech urządzeń Check Point 5600. Inżynier Wykonawcy otwierając zgłoszenie do producenta, oprócz posiadania ww. pakietu, powinien posiadać certyfikat CCSE (Expert) lub CCSM (Master) umożliwiający eskalację zgłoszeń serwisowych. W przypadku gdy producent nie oferuje supportu do końca okresu trwania umowy, Wykonawca wykupi przedłużenie supportu producenta na okres maksymalnie

dostępny, a w pozostałym czasie obowiązywania umowy Wykonawca zapewni support we własnym zakresie.

Identyfikator	U-LAN-011
----------------------	------------------

Wykonawca zakupi przedłużenie do końca okresu trwania umowy supportu producenta dla czterech (4) urządzeń F5 Big-IP i4800. Obecne aktywne moduły Local Traffic Manager, i4800 (Perpetual) Data Licencji Nov 27, 2020.

14. Wymagania na rozwój środowiska sieciowego LAN

Identyfikator	R-LAN-001
----------------------	------------------

Dostarczenie, instalacja oraz konfiguracja przez Wykonawcę dwóch (2) urządzeń typu firewall (wymiana dwóch istniejących firewall Palo Alto PA3020) na urządzenia o parametrach nie gorszych od obecnego rozwiązania.

- Wykonawca musi zainstalować dodatkowe licencje: Threat prevention i URL filtering.
- Wykonawca przeniesie obecną konfigurację z posiadanych przez Zamawiającego urządzeń na dostarczone przez Wykonawcę.
- Wykonawca skonfiguruje weryfikację podłączonych użytkowników i ich statusu w systemie monitoringu.
- Wykonawca dokona odpowiedniej modyfikacji oprogramowania (które jest obecnie wykorzystywane przez zamawiającego na PA3020) umożliwiającego szybkie zarządzanie udzielanym dostępem vpn dla użytkowników.
- Wykonawca dostarczy niezbędne okablowanie.
- Zamawiający wymaga wykupienia przez Wykonawcę supportu producenta (na okres trwania umowy) części sprzętowej i programowej urządzeń w formacie „Next Business Day”.

Wymagania dla dwóch (2) urządzeń firewall:

- Urządzenia muszą pracować w klastrach w architekturze wysokiej dostępności w trybie failover (active/passive) z realizacją HA w oparciu o sprzęt fizyczny.
- Urządzenie musi być dostarczone jako dedykowane urządzenie typu appliance, przystosowane do montażu w szafie Rack 19” o wysokości 1U.
- Urządzenie musi być wyposażone w twardego dysku SSD do przechowywania logów i raportów o pojemności nie mniejszej niż 120 GB.
- Urządzenie musi być wyposażone w dedykowany port konsoli/zarządzania. Port ten musi być wydzielony co najmniej logicznie i musi pracować w innej instancji routingu co porty obsługujące ruch poddawany inspekcji.
- Urządzenie musi być wyposażone w 8 interfejsów 100/1000/10GE Ethernet (RJ45) oraz 4 interfejsy 1/10GE SFP+.
- Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe:
 - Minimum 8,6 Gbps dla Firewall/kontroli aplikacji
 - Minimum 3,2 Gbps dla Firewall/IPS/Antywirus/kontroli aplikacji/Antymalware
 - Minimum 100 tys. nowych sesji na sekundę.
- Urządzenie musi obsługiwać protokół Ethernet z obsługą sieci VLAN. Urządzenie musi obsługiwać 4094 znaczników VLAN zgodnych z 802.1q. Urządzenie musi pozwalać na tworzenie tzw. subinterfejsów na interfejsach pracujących w trybie L2 i L3.

- Urządzenie musi umożliwiać translację adresów IP (NAT) zarówno statyczną jak i dynamiczną. Reguły dotyczące NAT muszą być odrębne od reguł definiujących polityki bezpieczeństwa tak aby reguły dotyczące translacji nie powodowały w żaden sposób zależności od konfiguracji tych polityk.
- Urządzenie musi obsługiwać co najmniej 1500 tuneli IPSEC VPN z wydajnością minimum 4.6 Gbps. Jeżeli wykorzystanie funkcji remote VPN (IPSec i SSL) wymaga zakupu dodatkowych licencji, lub jeżeli dedykowany klient VPN oferowany przez producenta firewall wymaga zakupu dodatkowych licencji to należy je przewidzieć w ofercie dla maksymalnej obsługiwanej przez urządzenie ilości użytkowników.
- Urządzenie musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
- Urządzenie musi umożliwiać obsługę protokołów routingu minimum RIP, OSPF oraz BGP.
- Urządzenie musi wspierać mechanizm PBR (policy base routing) dla wybranych aplikacji i wskazanych użytkowników – mechanizm przekierowania ruchu z pominięciem tablicy routingu.
- Urządzenie musi umożliwiać obsługę klastra niezawodnościowego – tworzenia konfiguracji odpornej na awarie dla urządzeń. Urządzenia w klastrze muszą funkcjonować w trybie Active/Passive i Active/Active.
- Polityka bezpieczeństwa systemu zabezpieczeń musi prowadzić kontrolę ruchu sieciowego i uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, kategorie URL reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem QoS. Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 1500 reguł polityki bezpieczeństwa.
- Urządzenie musi umożliwiać rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. 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 firewalla stanowego i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż wskazano w wymaganiach wydajnościowych.
- Urządzenie musi wykrywać co najmniej 2500 predefiniowanych aplikacji wspieranych przez producenta (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi.
- Urządzenie musi przeprowadzać kontrolę aplikacji w sposób umożliwiający potraktowanie informacji o niej jako atrybutu a nie jako wartości w polityce bezpieczeństwa. W szczególności dotyczy to implementacji w modułach innych jak firewall (np. w IPS lub innym module UTM) w których informacja o aplikacji będzie mogła być tylko wykorzystana jako „wartość” w polityce.
- Urządzenie musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (antywirus, IPS, URL, blokowanie plików) per aplikacja. Urządzenie musi posiadać możliwość przydzielania innych profili ochrony (AV, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.
- Urządzenie musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.
- Urządzenie musi pozwalać na 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.

- Urządzenie musi posiadać funkcjonalność dekrypcji SSL w tym możliwość zdefiniowania ruchu SSL który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.
- Urządzenie musi posiadać funkcjonalność Intrusion Prevention System (IPS) wraz z aktualizacją sygnatur w okresie gwarancji. System IPS musi działać w warstwie 7 modelu OSI. Baza sygnatur musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co urządzenie.
- Urządzenie musi posiadać funkcjonalność Antywirus (AV) wraz z aktualizacją sygnatur w okresie gwarancji. Moduł AV musi być uruchamiany per aplikacja oraz wybrany dekodery taki jak http, smtp, imap, pop3, ftp, smb.
Baza sygnatur AV musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
- Urządzenie musi zapewniać ochronę przed atakami typu Spyware – Zamawiający dopuszcza by odbywało się to poprzez silnik AV lub silnik IPS lub silnik antymalware lub dedykowany silnik antyspyware.
- Urządzenie musi posiadać narzędzia wykrywające i blokujące ruch do domen uznanych za złośliwe (sygnatury DNS). Rozwiązanie musi umożliwiać podmianę 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).
- Urządzenie musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.
- Urządzenie musi posiadać funkcjonalność URL Filtering wraz z aktualizacją w okresie gwarancji.
- Zarządzanie urządzeniem musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW.
- Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji).
- Urządzenie musi umożliwiać eksportowanie logów do zewnętrznych serwerów SYSLOG.
- Urządzenie musi być wyposażone w zasilacze typu AC pracujące redundantnie.

Identyfikator	R-LAN-002
---------------	-----------

Dostarczenie, wymiana oraz konfiguracja platformy czterech (4) routerów wewnętrznych.

Wykonawca dokona wymiany i konfiguracji obecnie pracujących czterech (4) routerów Juniper J6350 pełniących rolę routerów wewnętrznych (po dwa na lokalizację) - zapewniających łączność pomiędzy lokalizacjami.

- Konfiguracja urządzeń przez Wykonawcę, przeniesienie obecnej konfiguracji z posiadanych przez Zamawiającego urządzeń na dostarczone przez Wykonawcę. Zestawienie tuneli VPN do drugiej lokalizacji oraz konfiguracja weryfikacji ich statusu w systemie monitoringu
- Dostarczenie niezbędnego okablowania.
- Zamawiający wymaga wykupienia przez Wykonawcę supportu producenta (na okres trwania umowy) części sprzętowej i programowej urządzeń w formacie „Next Business Day”.

Wymagania na routery wewnętrzne:

- Urządzenie musi być dostarczone jako dedykowane urządzenie sieciowe o wysokości 1U.
- Urządzenie musi być wyposażone w redundantny zasilacz dostosowany do napięcia zmiennego 220-230V.
- Urządzenie musi być wyposażone w co najmniej 4 GB pamięci RAM, pamięć Flash 8 GB oraz port konsoli. Urządzenie musi posiadać slot USB przeznaczony do podłączenia dodatkowego nośnika danych. Musi być dostępna opcja uruchomienia systemu operacyjnego z nośnika danych podłączonego do slotu USB na module kontrolnym.
- Urządzenie musi posiadać dodatkowy slot SSD na umieszczenie dysku typu SSD.
- System operacyjny urządzenia musi posiadać budowę modułową (moduły muszą działać w odseparowanych obszarach pamięci) i zapewniać całkowitą separację płaszczyzny kontrolnej od płaszczyzny przetwarzania ruchu użytkowników.
- System operacyjny urządzenia musi śledzić stan sesji połączeń (stateful processing), tworzyć i zarządzać tablicą stanu sesji. Musi istnieć opcja przełączenia urządzenia w tryb pracy bez śledzenia stanu sesji, jak również wyłączenia części ruchu ze śledzenia stanu sesji.
- Urządzenie musi być wyposażone w nie mniej niż 8 wbudowanych interfejsów Ethernet 10/100/1000 (gotowych do użycia bez konieczności zakupu dodatkowych modułów i licencji).
- Urządzenie musi realizować zadania Stateful Firewall z mechanizmami ochrony przed atakami DoS, wykonując kontrolę na poziomie sieci 1,5 Gbps liczoną dla ruchu IMIX. Urządzenie musi obsłużyć nie mniej niż 350 000 równoległych sesji oraz zestawić nie mniej niż 15 000 nowych połączeń na sekundę.
- Urządzenie musi zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. IPSec VPN musi być realizowany sprzętowo. Urządzenie musi obsługiwać nie mniej niż 2 000 równoległych tuneli VPN oraz ruch szyfrowany o przepustowości nie mniej niż 320 Mb/s dla ruchu IMIX.
- Urządzenie musi obsługiwać protokoły dynamicznego routingu: RIP, OSPF oraz BGP. Urządzenie musi umożliwiać skonfigurowanie nie mniej niż 60 wirtualnych ruterów. Tablica routingu powinna umożliwiać utrzymanie 1 miliona wpisów routingu natomiast tablica forwardingu minimum 600 000 tras.
- Urządzenie musi umożliwiać edycję konfiguracji wykonywalnej bez natychmiastowego jej uruchamiania, blokowe uruchamianie zmian konfiguracyjnych, cofanie zmian konfiguracyjnych do poprzedniej wersji, a także automatyczne cofnięcie się do poprzedniej wersji konfiguracji w przypadku np. utraty łączności administracyjnej z urządzeniem w wyniku ostatniej wprowadzonej zmiany.
- Urządzenie musi być kompatybilne z systemem zarządzania siecią Junos Space.

Identyfikator

R-LAN-003

Dostarczenie, instalacja oraz konfiguracja przez Wykonawcę czterech (4) przełączników (wymiana istniejących przełączników EX4200, po dwa (2) w każdej lokalizacji), obsługujące strefę LAN. Przełączniki będą obsługiwać połączenia logiczne dla sieci IP w strefie Back End i muszą być połączone w stos.

Wymagania na cztery (4) przełączniki 48-portowe bez PoE z opcją stackowania do pracy w strefie LAN:

- Przełącznik musi być dedykowanym urządzeniem sieciowym o wysokości nie większej niż 1U przystosowanym do montowania w szafie rack 19 cali, wyposażonym w wymienne zasilacze oraz wentylatory.

- Urządzenie musi być wyposażone w redundantny zasilacz dostosowany do napięcia zmiennego 220-230V.
- Urządzenie musi być chłodzone przepływem powietrza w schemacie od przodu do tyłu. Za przód urządzenia przyjmuje się stronę z zabudowanymi interfejsami tranzytowymi 1 oraz 10Gbps.
- Przełącznik musi mieć przepustowość nie mniejszą niż 376 Gbps oraz obsługiwać nie mniej niż 279 Mpps (milionów pakietów na sekundę) - przepustowości nieblokujące dla wszystkich wymaganych specyfikacją portów.
- Przełącznik musi być wyposażony co najmniej w 48 portów 1 Gigabit Ethernet RJ-45.
- Przełącznik musi być wyposażony co najmniej w 4 porty 1/10 Gigabit Ethernet (oddzielne od wymienionych w poprzednim podpunkcie). Typ złącza interfejsu musi być określany przez wymienny moduł SFP+.
- Przełącznik musi być wyposażony co najmniej w 4 porty 10/25 Gigabit Ethernet (oddzielne od wymienionych w poprzednich podpunktach). Typ złącza interfejsu musi być określany przez wymienny moduł SFP28.
- Wraz z przełącznikiem muszą zostać dostarczone następujące interfejsy wymienne 2x 25Gbps: 25GBase-SR.
- Przełącznik musi być wyposażony w co najmniej jeden interfejs zarządzania OOB GE 1GBase-T RJ-45 oraz port szeregowy konsoli zarządzającej.
- Urządzenie musi wspierać agregację linków Ethernet, statyczną oraz z wykorzystaniem protokołu LACP, min. 8 portów per grupa oraz minimum 128 różnych grup per zagregowana grupa urządzeń.
- Urządzenie musi jednocześnie obsługiwać sprzętowo nie mniej niż 64 tysięcy wpisów w tablicy adresów MAC i 32 tysięcy wpisów w tablicy ARP.
- Urządzenie musi posiadać funkcję filtrowania ruchu wchodzącego i wychodzącego z wszystkich interfejsów (ACL). Filtrowanie musi odbywać się co najmniej na podstawie adresów MAC oraz IPv4/IPv6 łącznie tzn. pojedyncza definicja ACE (access control entry) może objąć zarówno nagłówki L2 jak i L3. Włączenie filtrowania nie może powodować degradacji wydajności urządzenia, tzn. musi być realizowane sprzętowo z prędkością łącza.
- Urządzenie musi wspierać protokół 802.1X w celu uwierzytelnienia dołączonego suplikanta (pojedynczego lub większej liczby per interfejs) na serwerze RADIUS oraz akceptować co najmniej przypisanie vlan-u oraz grup SGT jako wyniku procesu autoryzacji. Dla urządzeń klienckich bez oprogramowania suplikanta, urządzenie musi wykonać uwierzytelnienie wykorzystując adres MAC.
- Urządzenie musi umożliwiać edycję konfiguracji wykonywalnej na urządzeniu bez natychmiastowego jej uruchamiania, blokowe uruchamianie zmian konfiguracyjnych, cofanie zmian konfiguracyjnych do poprzedniej wersji, a także automatyczne cofnięcie się do poprzedniej wersji konfiguracji w przypadku np. utraty łączności administracyjnej z urządzeniem w wyniku ostatniej wprowadzonej zmiany.
- Urządzenie musi być kompatybilne z systemem zarządzania siecią Junos Space.

Urządzenie musi mieć możliwość pracy jako pojedynczy, administrowany z pojedynczej konsoli i pod wspólnym adresem IP przełącznik logiczny w grupie do 10 urządzeń; dystans pomiędzy poszczególnymi urządzeniami fizycznymi może przekraczać 100m. Jeżeli funkcjonalność ta wymaga dodatkowego licencjonowania, to licencje te muszą zostać dostarczone wraz z urządzeniem.

Identyfikator	R-LAN-004
<p>Wykonawca dostarczy, zainstaluje i skonfiguruje jedno (1) urządzenie firewall do Centrali UAE (ul. Giełdowa 7/9).</p>	
<ul style="list-style-type: none"> • Konfiguracja urządzeń przez Wykonawcę, przeniesienie obecnej konfiguracji z posiadanych przez Zamawiającego urządzeń na dostarczone przez Wykonawcę. Zestawienie tuneli VPN z Centrali do lok. Borucza i Siemianowice Śl. oraz konfiguracja weryfikacji ich statusu w systemie monitoringu. • Dostarczenie niezbędnego okablowania. • Zamawiający wymaga wykupienia przez Wykonawcę supportu producenta (na okres trwania umowy) części sprzętowej i programowej urządzeń w formie „Next Business Day”. 	
<p>Wymagania na urządzenie :</p>	
<ul style="list-style-type: none"> • Firewall musi być dostarczony jako dedykowane urządzenie sieciowe o wysokości 1U. • Urządzenie musi być wyposażone w zasilacz dostosowany do napięcia zmiennego 220-230V. • Urządzenie musi posiadać elementy do montażu w szafie rack 19’. • Urządzenie musi być wyposażone w co najmniej 4 GB pamięci RAM, pamięć Flash 8 GB oraz port konsoli. Urządzenie musi posiadać slot USB przeznaczony do podłączenia dodatkowego nośnika danych. Musi być dostępna opcja uruchomienia systemu operacyjnego z nośnika danych podłączonego do slotu USB na module kontrolnym. • System operacyjny urządzenia musi posiadać budowę modułową (moduły muszą działać w odseparowanych obszarach pamięci) i zapewniać całkowitą separację płaszczyzny kontrolnej od płaszczyzny przetwarzania ruchu użytkowników. • System operacyjny urządzenia musi śledzić stan sesji połączeń (stateful processing), tworzyć i zarządzać tablicą stanu sesji. Musi istnieć opcja przełączenia urządzenia w tryb pracy bez śledzenia stanu sesji, jak również wyłączenia części ruchu ze śledzenia stanu sesji. • Urządzenie musi być wyposażone w nie mniej niż 6 wbudowanych interfejsów Ethernet 10/100/1000 (gotowych do użycia bez konieczności zakupu dodatkowych modułów i licencji). • Wbudowane porty 1GbE muszą umożliwiać korzystanie z funkcji PoE+. • Firewall musi realizować zadania Stateful Firewall z mechanizmami ochrony przed atakami DoS, wykonując kontrolę na poziomie sieci 600 Mbps liczoną dla ruchu IMIX. Urządzenie musi obsłużyć nie mniej niż 60 000 równoległych sesji oraz zestawień nie mniej niż 5 000 nowych połączeń na sekundę. • Firewall musi zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. IPSec VPN musi być realizowany sprzętowo. Urządzenie musi obsługiwać nie mniej niż 250 równoległych tuneli VPN oraz ruch szyfrowany o przepustowości nie mniejszej niż 100 Mb/s dla ruchu IMIX. • Urządzenie musi umożliwiać edycję konfiguracji wykonywalnej na urządzeniu bez natychmiastowego jej uruchamiania, blokowe uruchamianie zmian konfiguracyjnych, cofanie zmian konfiguracyjnych do poprzedniej wersji, a także automatyczne cofnięcie się do poprzedniej wersji konfiguracji w przypadku np. utraty łączności administracyjnej z urządzeniem w wyniku ostatniej wprowadzonej zmiany. • Urządzenie musi być kompatybilne z systemem zarządzania siecią Junos Space. 	

Identyfikator	R-LAN-005
<p>Dostarczenie, instalacja oraz konfiguracja przez wykonawcę sześciu (6) przełączników (wymiana z istniejących przełączników EX4200 i konfiguracja nowych po trzy (3) w stosie w każdej lokalizacji), obsługujące strefę DMZ.</p> <p>Ze względu na część urządzeń wymagających zasilania PoE część przełączników musi posiadać możliwość zasilania portów LAN.</p>	
<p>Wymagania, na 4 przełączniki 48-portowe bez PoE z opcją stackowania do pracy w strefie DMZ:</p> <ul style="list-style-type: none"> • Przełącznik musi być dedykowanym urządzeniem sieciowym o wysokości nie większej niż 1U przystosowanym do montowania w szafie rack 19 cali, wyposażonym w wymienne zasilacze oraz wentylatory. • Urządzenie musi być wyposażone w redundantny zasilacz dostosowany do napięcia zmiennego 220-230V. • Urządzenie musi być chłodzone przepływem powietrza w schemacie od przodu do tyłu. Za przód urządzenia przyjmuje się stronę z zabudowanymi interfejsami tranzytowymi 1 oraz 10Gbps. • Przełącznik musi mieć przepustowość nie mniejszą niż 376 Gbps oraz obsługiwać nie mniej niż 279 Mpps (milionów pakietów na sekundę) - przepustowości nieblokujące dla wszystkich wymaganych specyfikacją portów. • Przełącznik musi być wyposażony co najmniej w 48 portów 1 Gigabit Ethernet RJ-45. • Przełącznik musi być wyposażony co najmniej w 4 porty 1/10 Gigabit Ethernet (oddzielne od wymienionych w poprzednim podpunkcie). Typ złącza interfejsu musi być określany przez wymienny moduł SFP+. • Przełącznik musi być wyposażony co najmniej w 4 porty 10/25 Gigabit Ethernet (oddzielne od wymienionych w poprzednich podpunktach). Typ złącza interfejsu musi być określany przez wymienny moduł SFP28. • Wraz z przełącznikiem muszą zostać dostarczone następujące interfejsy wymienne 2x 25Gbps: 25GBase-SR. • Przełącznik musi być wyposażony w co najmniej jeden interfejs zarządzania OOB GE 1GBase-T RJ-45 oraz port szeregowy konsoli zarządzającej. • Urządzenie musi wspierać agregację linków Ethernet, statyczną, oraz z wykorzystaniem protokołu LACP, min. 8 portów per grupa, oraz minimum 128 różnych grup per zagregowana grupa urządzeń. • Urządzenie musi jednocześnie obsługiwać sprzętowo nie mniej niż 64 tysiące wpisów w tablicy adresów MAC i 32 tysiące wpisów w tablicy ARP. • Urządzenie musi posiadać funkcję filtrowania ruchu wchodzącego i wychodzącego z wszystkich interfejsów (ACL). Filtrowanie musi odbywać się co najmniej na podstawie adresów MAC oraz IPv4/IPv6 łącznie, tzn. pojedyncza definicja ACE (access control entry) może objąć zarówno nagłówki L2 jak i L3. Włączenie filtrowania nie może powodować degradacji wydajności urządzenia, tzn. musi być realizowane sprzętowo z prędkością łącza. • Urządzenie musi wspierać protokół 802.1X w celu uwierzytelnienia dołączonego suplikanta (pojedynczego lub większej liczby per interfejs) na serwerze RADIUS, oraz akceptować co najmniej przypisanie vlan-u oraz grup SGT jako wyniku procesu autoryzacji. Dla urządzeń klienckich bez oprogramowania suplikanta, urządzenie musi wykonać uwierzytelnienie wykorzystując adres MAC. 	

- Urządzenie musi umożliwiać edycję konfiguracji wykonywalnej na urządzeniu bez natychmiastowego jej uruchamiania, blokowe uruchamianie zmian konfiguracyjnych, cofanie zmian konfiguracyjnych do poprzedniej wersji, a także automatyczne cofnięcie się do poprzedniej wersji konfiguracji w przypadku np. utraty łączności administracyjnej z urządzeniem w wyniku ostatniej wprowadzonej zmiany.
- Urządzenie musi być kompatybilne z systemem zarządzania siecią Junos Space.
- Urządzenie musi mieć możliwość pracy jako pojedynczy, administrowany z pojedynczej konsoli i pod wspólnym adresem IP przełącznik logiczny w grupie do 10 urządzeń; dystans pomiędzy poszczególnymi urządzeniami fizycznymi może przekraczać 100m. Jeżeli funkcjonalność ta wymaga dodatkowego licencjonowania, to licencje te muszą zostać dostarczone wraz z urządzeniem. Wymagana jest możliwość połączenia z przełącznikami DMZ z PoE.

Wymagania na dwa (2) przełączniki 48-portowe z PoE z opcją stackowania do pracy w strefie DMZ:

- Przełącznik musi być dedykowanym urządzeniem sieciowym o wysokości nie większej niż 1U przystosowanym do montowania w szafie rack 19 cali, wyposażonym w wymienne zasilacze oraz wentylatory.
- Urządzenie musi być wyposażone w redundantny zasilacz dostosowany do napięcia zmiennego 220-230V.
- Urządzenie musi być chłodzone przepływem powietrza w schemacie od przodu do tyłu. Za przód urządzenia przyjmuje się stronę z zabudowanymi interfejsami tranzytowymi 1 oraz 10Gbps.
- Przełącznik musi mieć przepustowość nie mniejszą niż 376 Gbps oraz obsługiwać nie mniej niż 279 Mpps (milionów pakietów na sekundę) - przepustowości nieblokujące dla wszystkich wymaganych specyfikacją portów.
- Przełącznik musi być wyposażony co najmniej w 48 portów 1 Gigabit Ethernet RJ-45 z obsługą PoE do poziomu 30W na port i budżetem mocy 1440W.
- Przełącznik musi być wyposażony co najmniej w 4 porty 1/10 Gigabit Ethernet (oddzielne od wymienionych w poprzednim podpunkcie). Typ złącza interfejsu musi być określany przez wymienny moduł SFP+.
- Przełącznik musi być wyposażony co najmniej w 4 porty 10/25 Gigabit Ethernet (oddzielne od wymienionych w poprzednich podpunktach). Typ złącza interfejsu musi być określany przez wymienny moduł SFP28.
- Wraz z przełącznikiem muszą zostać dostarczone następujące interfejsy wymienne: 2x 25Gbps: 25GBase-SR.
- Przełącznik musi być wyposażony w co najmniej jeden interfejs zarządzania OOB GE 1GBase-T RJ-45 oraz port szeregowy konsoli zarządzającej.
- Urządzenie musi wspierać agregację linków Ethernet, statyczną oraz z wykorzystaniem protokołu LACP, min. 8 portów per grupa oraz minimum 128 różnych grup per zagregowana grupa urządzeń.
- Urządzenie musi jednocześnie obsługiwać sprzętowo nie mniej niż 64 tysiące wpisów w tablicy adresów MAC i 32 tysiące wpisów w tablicy ARP.
- Urządzenie musi posiadać funkcję filtrowania ruchu wchodzącego i wychodzącego z wszystkich interfejsów (ACL). Filtrowanie musi odbywać się co najmniej na podstawie adresów MAC oraz IPv4/IPv6 łącznie, tzn. pojedyncza definicja ACE (access control entry) może objąć zarówno

nagłówki L2 jak i L3. Włączenie filtrowania nie może powodować degradacji wydajności urządzenia, tzn. musi być realizowane sprzętowo z prędkością łącza.

- Urządzenie musi wspierać protokół 802.1X w celu uwierzytelnienia dołączonego suplikanta (pojedynczego lub większej liczby per interfejs) na serwerze RADIUS oraz akceptować co najmniej przypisanie vlan-u oraz grup SGT jako wyniku procesu autoryzacji. Dla urządzeń klienckich bez oprogramowania suplikanta, urządzenie musi wykonać uwierzytelnienie wykorzystując adres MAC.
- Urządzenie musi umożliwiać edycję konfiguracji wykonywalnej na urządzeniu bez natychmiastowego jej uruchamiania, blokowe uruchamianie zmian konfiguracyjnych, cofanie zmian konfiguracyjnych do poprzedniej wersji, a także automatyczne cofnięcie się do poprzedniej wersji konfiguracji w przypadku np. utraty łączności administracyjnej z urządzeniem w wyniku ostatniej wprowadzonej zmiany.
- Urządzenie musi mieć możliwość pracy jako pojedynczy, administrowany z pojedynczej konsoli i pod wspólnym adresem IP przełącznik logiczny w grupie do 10 urządzeń; dystans pomiędzy poszczególnymi urządzeniami fizycznymi może przekraczać 100m. Jeżeli funkcjonalność ta wymaga dodatkowego licencjonowania, to licencje te muszą zostać dostarczone wraz z urządzeniem. Wymagana jest możliwość połączenia z przełącznikami DMZ bez PoE.

15. Wymagania na utrzymanie środowiska bazodanowego BD

Serwery i oprogramowanie bazodanowe

Identyfikator	U-BD-001
Wykonawca co najmniej dwa (2) razy do roku przeprowadzi przegląd środowiska bazodanowego, obejmujący:	
<ul style="list-style-type: none">• Przegląd zawartości plików zdarzeń log na wszystkich serwerach bazodanowych wraz z ich analizą i rozwiązaniem problemów zidentyfikowanych na bazie plików log (m.in. pliki zdarzeń log samego systemu operacyjnego wraz z plikami zdarzeń log dla zainstalowanych baz danych).• Wykonanie testów bezpieczeństwa w celu wykrycia podatności wraz z usunięciem wykrytych podatności na wszystkich serwerach bazodanowych, co zostanie potwierdzone ponownymi testami środowiska bazodanowego.• Wykonane testy, usunięcie luk oraz ponowne testy, Wykonawca udokumentuje w przekazanej Zamawiającemu dokumentacji. Przekazana dokumentacja zawierać będzie m.in. szczegółowy opis (instrukcję) usuwania wykrytych podatności.• Przetestowanie a następnie wdrożenie dostępnych uaktualnień dla oprogramowania bazodanowego.• Dokonanie analizy plików bazodanowych min. pod kątem integralności danych, weryfikację poziomu defragmentacji indeksów bazodanowych. W przypadku stwierdzenia błędów lub nieprawidłowości Wykonawca wdroży odpowiednie działania naprawcze.• Weryfikacja poprawności importu danych z baz produkcyjnych do bazy raportowej. W przypadku stwierdzenia błędów lub nieprawidłowości Wykonawca wdroży odpowiednie działania naprawcze.• W przypadku wygaśnięcia wsparcia od producenta oprogramowania, Wykonawca zakupi odpowiednią ilość licencji i wdroży aktualizację do wersji aktualnie wspieranej.• Po realizacji wymagania Zamawiającemu dostarczony zostanie szczegółowy raport z wykonanych prac.	

Oprogramowanie IBM InfoSphere Guardium do monitorowania baz danych DAM (ang. Database Activity Monitor)

Identyfikator	U-BD-002
<p>Wykonawca co najmniej dwa (2) razy do roku przeprowadzi przegląd systemów IBM InfoSphere Guardium (w skrócie Guardium), obejmujący:</p> <ul style="list-style-type: none">• Przegląd zawartości plików zdarzeń na wszystkich komponentach wchodzących w skład systemu Guardium wraz z ich analizą i rozwiązaniem zidentyfikowanych problemów.• Przegląd i analiza wykrytych przez system Guardium incydentów i anomalii oraz podjęcie ewentualnych działań naprawczych.• Przetestowanie a następnie wdrożenie dostępnych uaktualnień dla wszystkich komponentów oprogramowania Guardium .• W przypadku wygaśnięcia wsparcia od producenta oprogramowania, Wykonawca zakupi odpowiednią ilość licencji i wdroży aktualizację do wersji aktualnie wspieranej.• Po realizacji wymagania Zamawiającemu dostarczony zostanie szczegółowy raport z wykonanych prac.	

Identyfikator	U-BD-003
<p>Wykonawca wykupi wsparcie producenta dla czterech instancji IBM InfoSphere Guardium na czas trwania umowy.</p> <p>W przypadku wygaśnięcia wsparcia od producenta oprogramowania, Wykonawca zakupi odpowiednią ilość licencji i wdroży aktualizację do wersji aktualnie wspieranej. Po wdrożonej aktualizacji żaden z elementów Systemu PLI CBD nie może ulec pogorszeniu ze względu na szybkość i niezawodność działania. Jeżeli utrzymanie dotychczasowych parametrów wydajnościowych będzie wiązało się z koniecznością doposażenia lub wymiany sprzętu, Wykonawca dokona stosownych zakupów i je wdroży.</p> <p>Wykonawca wykaże iż wsparcie producenta oprogramowania nie wygaśnie w ciągu sześciu (6) miesięcy od zakończenia obowiązywania umowy. Jeżeli do sześciu (6) miesięcy od daty zakończenia umowy miałyby wygasnąć wsparcie producenta oprogramowania, Wykonawca zakupi i wdroży odpowiednią aktualizację przed zakończeniem czasu trwania umowy z zastrzeżeniem identycznych warunków jak dla zakończenia wsparcia w czasie obowiązywania umowy.</p> <p>Jeżeli wykupienie nowej wersji oprogramowania nie będzie możliwe to wykonawca zaproponuje dostarczenie nowego oprogramowania o parametrach nie gorszych niż obecnie zainstalowane rozwiązanie. Wykonawca przed dostarczeniem nowego rozwiązania musi przedstawić do akceptacji Zamawiającego analizę porównawczą parametrów oferowanego systemu DAM do obecnie zainstalowanego w PLI CBD.</p> <p>Zamawiający zastrzega sobie prawo do odrzucenia zaproponowanego rozwiązania w przypadku ujawnienia gorszych parametrów w nowym rozwiązaniu względem obecnego.</p>	

System Centralnej kolekcji i korelacji zdarzeń - Oprogramowanie RSA enVision.

Identyfikator	U-BD-004
<p>Wykonawca co najmniej dwa (2) razy do roku przeprowadzi przegląd systemów RSA enVision, obejmujący:</p> <ul style="list-style-type: none"> • Przegląd zawartości plików zdarzeń na wszystkich komponentach wchodzących w skład systemu RSA enVision wraz z ich analizą i rozwiązaniem zidentyfikowanych problemów. • Przegląd procesu importu logów w tym zainstalowanych analizatorów składni (parserów), pod kątem aktualności zbieranych logów z systemu PLI CBD. W przypadku wykrycia nieprawidłowości Wykonawca dokona niezbędnych działań naprawczych i aktualizacji. • Po realizacji wymagania Zamawiającemu dostarczony zostanie szczegółowy raport z wykonanych prac. 	

Identyfikator	U-BD-005
<ul style="list-style-type: none"> • W przypadku dokonania zmian w modułach aplikacji PLI CBD, powodujących generowanie nowego typu logów aplikacyjnych, Wykonawca dokona niezbędnych uaktualnień w systemie centralnej kolekcji i korelacji zdarzeń min. zaktualizuje zainstalowane analizatory składni (parsery), zaimportuje nowe typy logów. • Uaktualnienia zostaną zrealizowane w ciągu 7 dni od dokonania zmian w modułach aplikacji PLI CBD. • Po realizacji wymagania Zamawiającemu dostarczony zostanie szczegółowy raport z wykonanych prac. 	

16. Wymagania na utrzymanie Aplikacji PLI CBD

Identyfikator	U-APP-001
<p>Wykonawca zobowiązany jest utrzymywać i aktualizować na zasobach Zamawiającego repozytorium kodów źródłowych Aplikacji PLI CBD. Zamawiający dysponuje repozytorium kodów GitLab. Repozytorium posiada mechanizmy kontroli wersji, a także rozdzielania (ang. <i>branch</i>) kodów na kilka równoległych ścieżek powstawania i scalania (ang. <i>merge</i>) tych ścieżek z powrotem w jedną ścieżkę. Zawiera kody źródłowe wszystkich komponentów programowych Aplikacji PLI CBD oraz baz danych, w tym: procedury, pliki konfiguracyjne, skrypty itd. Wszystkie aktualizacje i poprawki, a także wdrożenia w ramach rozwoju wprowadzane w toku trwania umowy będą miały odzwierciedlenie we wspomnianym repozytorium, będą udokumentowane i będą posiadać odpowiednie komentarze. Wdrażane aplikacje będą budowane w oparciu o skompilowany kod z GitLab. Instalacja odbywa się najpierw na środowisku testowym, a po akceptacji Zamawiającego na środowisku produkcyjnym. Zarządzanie procesem będzie odbywać się zgodnie z aktualnymi procedurami: Techniczną instrukcją i wskazówki zarządzania kodem dla Wykonawcy oraz Instrukcją instalacji/wdrożenia wersji systemu PLI CBD.</p>	

Identyfikator	U-APP-002
<p>Raz (1) do roku Wykonawca przygotowuje listę i opis zmian Systemu PLI CBD wynikających ze zmian prawnych, co obejmie:</p> <ul style="list-style-type: none"> • Dodawanie nowych funkcjonalności. • Modyfikację istniejących funkcjonalności. • Skasowanie nieaktualnych funkcjonalności. <p>Wykonawca przeprowadzi analizę przepisów obowiązującego prawa w szczególności dotyczącego:</p> <ul style="list-style-type: none"> • Prawa telekomunikacyjnego. 	

- Ochrony danych osobowych i stosowanych rozporządzeń.
- Bezpieczeństwa teleinformatycznego.
- Budowania systemów teleinformatycznych w administracji publicznej.

Analiza ma być wykonana zarówno na poziomie ruchu głosowego, jak i ruchu sygnalizacyjnego. Wykonawca zobowiązany jest do uwzględnienia wymiany ruchu pomiędzy operatorami telekomunikacyjnymi (w tym również do numerów przeniesionych) i związanych z tym obowiązków operatorów telekomunikacyjnych zarówno w odniesieniu do usług stacjonarnych, jak i ruchomych. Podsumowaniem tych prac będzie dokumentacja opisująca wymagane zmiany w Systemie PLI CBD.

Identyfikator	U-APP-003
<p>Wykonawca co najmniej dwa (2) razy do roku przeprowadzi przegląd środowiska aplikacyjnego produkcyjnego oraz testowego PLI CBD obejmujący:</p>	
<ul style="list-style-type: none"> • Przegląd zawartości plików zdarzeń aplikacji PLI CBD wraz z ich analizą i rozwiązaniem problemów zidentyfikowanych podczas przeglądu. • Przegląd zawartości plików zdarzeń serwerów IIS wraz z ich analizą i rozwiązaniem problemów zidentyfikowanych podczas przeglądu. • Przegląd zawartości baz danych pod kątem zawartości błędów aplikacji. • Przedstawienie statystyk występowania różnych rodzajów błędów. • Sprawdzenie wersji zainstalowanych serwisów aplikacyjnych. • Porównanie wersji serwisów aplikacyjnych pomiędzy środowiskiem produkcyjnym i środowiskiem testowym. W przypadku wykrycia różnic w wersjach serwisów wyrównanie (uspójnienie) środowisk. • Archiwizacja modułów i elementów aplikacji PLI CBD wycofanych z produkcji (pliki wykonywalne, logi, usługi, serwisy webowe, elementy po stronie bazy danych w szczególności procedury zapamiętane). • Zbieranie statystyk z działania aplikacji PLI CBD – ilość zrealizowanych wniosków FNP, MNP, ilość zdarzeń lokalizacyjnych otrzymanych i wysłanych, ilość poszczególnych komunikatów NP, czas przetwarzania komunikatów, statystyki bazy numerów przeniesionych i numeracji udostępnianej. • Pomiar czasu przetwarzania, zapisu oraz przekazywania do służb zgłoszeń alarmowych związanych z usługą E112. • Pomiar czasu przetwarzania, zapisu i przekazywania paczek w ramach usługi NP. • Ocena trendów odnośnie czasu przetwarzania w stosunku do liczby zgłoszeń/paczek NP. • Na podstawie zebranych statystyk Wykonawca przedstawi potencjalne zagrożenia dotyczące wydajności i dostępności aplikacji i usług oraz integralności danych. • Sprawdzanie funkcjonowania i ewentualnych błędów replikacji i synchronizacji. • Przedstawienie propozycji rozwiązania zidentyfikowanych problemów. 	
<p>Po akceptacji zamawiającego wdrożenie zaproponowanych zmian eliminujących zidentyfikowane problemy.</p>	

Identyfikator	U-APP-004
<p>Wykonawca co najmniej dwa (2) razy do roku przeprowadzi testy bezpieczeństwa Aplikacji PLI CBD. Podczas testów należy sprawdzić odporność aplikacji na wszystkie typy ataków wymienionych na aktualnej liście OWASP Top 10.</p>	

Minimalny zakres prac:

- Analiza udostępnianych informacji przez Aplikację PLI CBD.
- Analiza wersji i konfiguracji zastosowanego oprogramowania.
- Próby wykrycia możliwych dostępu administracyjnych.
- Analiza mechanizmów uwierzytelniania i autoryzacji stosowanych w Aplikacji PLI CBD.
- Próby przełamania i ominięcia mechanizmów uwierzytelniania oferowanych przez Aplikację PLI CBD.
- Sprawdzenie trywialności haseł (ataki metodą słownikową).
- Manipulacja wartościami znajdującymi się w pliku cookie przesyłanym przez Aplikację PLI CBD.
- Analiza zabezpieczenia przesyłu identyfikatorów sesji.
- Próby odgadnięcia sposobu generowania identyfikatorów sesji.
- Próby podszycia się pod sesję innego użytkownika.
- Próby rozszerzenia nadanych uprawnień przez użytkowników.
- Próby uzyskania nieautoryzowanego dostępu do danych innych użytkowników.
- Analiza danych wysyłanych i odbieranych przez Aplikację PLI CBD.
- Próby manipulacji wartościami ukrytymi znajdującymi się w formularzach HTML.
- Analizę reakcji Aplikacji PLI CBD na wprowadzanie nieoczekiwanych lub nieprawidłowych danych.
- Próby destabilizacji pracy Aplikacji PLI CBD przy pomocy nieprawidłowych wartości w żądaniach.
- Próby destabilizacji Aplikacji PLI CBD przy pomocy nieprawidłowych wartości w nagłówkach protokołu http.
- Próby ataków: "Reflected/Stored/ Dom Based Cross-site scripting", "Cross Site Flashing", „Server Side Include", "SQL Injection", "CSRF", "XPATH Injection", "IMAP/SMTP Injection", "Code Injection", "OS Commanding", "Buffer Overflow", "HTTP Spliting/Smuggling", "Denial of Service".
- Analiza możliwości powtórnego przesyłania przechwyconych danych.
- Analiza błędów typowych dla wykorzystywanej przez Aplikację PLI CBD technologii.
- Weryfikacja szyfrowania danych przez Aplikację PLI CBD.
- Testowanie możliwości dostępu do usług sieciowych (zarówno faktycznie wykorzystywanych serwisów, jak i domyślnie otwartych i zapomnianych portów).
- Przeanalizowanie potencjalnych zagrożeń dla istniejących serwerów usług IIS (wersje systemów, wersje oprogramowania, otwarte porty, podatność na znane ataki).
- Przesyłanie odpowiednio spreparowanych oraz zainfekowanych plików XML do Aplikacji PLI CBD.
- W przypadku wykrytych podatności Wykonawca usunie je. W razie konieczności dokona stosownych zmian w Aplikacji PLI CBD. Przeprowadzi ponowny test weryfikujący poprawność usunięcia luk. Wykonane testy, usunięcie luk oraz ponowne testy, Wykonawca udokumentuje w przekazanej Zamawiającemu dokumentacji.

Identyfikator	U-APP-005
Na dwa (2) tygodnie przed dniem zakończenia umowy Wykonawca zobowiązany jest do przekazania Zamawiającemu:	
1. W zakresie kodu aplikacji:	
- aktualny kod aplikacji w podziale na poszczególne komponenty systemu, który umożliwił będzie jego kompilację,	
- aktualną dokumentację dla kodu źródłowego zawierającej minimum:	
o listę wszystkich klas i funkcji wraz z opisem parametrów wejściowych i wyjściowych,	
o listę bibliotek i kontrolek z wyszczególnieniem tych które wymagają wykupienia licencji u firm trzecich,	
o przepływ danych pomiędzy poszczególnymi komponentami systemu (w postaci diagramów) w tym szczegółowy wykaz operacji komunikacji z bazami danych	

- instrukcje kompilowania kodów źródłowych oraz instrukcje instalacje wytworzonych komponentów w środowisku oprogramowania standardowego,
 - opis parametrów konfiguracyjnych komponentów systemu.
2. W zakresie baz danych:
- o aktualnych skryptów umożliwiających utworzenie baz danych, tabel, widoków, synonimów, procedur składowanych i funkcji,
 - o aktualnej dokumentacji do baz danych, tabel, widoków, synonimów, procedur składowanych i funkcji,
 - o dokumentacja powinna zawierać minimum takie informacje jak: nazwy danych, typy, wartości domyślne, opis kluczy głównych i kluczy zewnętrznych, indexy, w przypadku procedur i funkcji wartości wejściowe i wyjściowe,
 - o instrukcje użycia skryptów z punktu pierwszego w celu wygenerowania zerowego* stanu systemu bazodanowego

W celu przeprowadzenia procedury odbioru kodów źródłowych wykonawca przy współudziale zamawiającego na trzy dni robocze przed końcem umowy w wyznaczonym CPD dokona kompilacji przekazanego kodu źródłowego zgodnie z przekazaną instrukcją, a następnie instalacji wytworzonych komponentów w środowisku testowym zamawiającego również zgodnie z przekazaną instrukcją.

*- bez danych

17. Wymagania na rozwój Aplikacji PLI CBD

Identyfikator	R-APP-001
<p>Zamawiający w czasie trwania umowy wymaga puli 50 Roboczodni, przeznaczonych na rozwój Systemu PLI CBD. Przeznaczone one będą na prace rozwojowe w zakresie Aplikacji PLI CBD oraz Infrastruktury Informatycznej. Tylko te wymagania umieszczone w niniejszym dokumencie Opisującym Przedmiot Zamówienia posiadające nadany Identyfikator w którym to wymaganiu wyraźnie zaznaczono, iż realizacja wymagania uszczupla pulę Roboczodni zmniejszając pulę Roboczodni po oczywistym zatwierdzeniu jej przez Zamawiającego i przekazaniu zadania do realizacji. W przeciwnym przypadku jeżeli takiego zapisu nie ma, to wymagane czynności realizowane w ramach realizacji przedmiotu zamówienia, poza pulą 50 Roboczodni. W niektórych wymaganiach dodatkowo, wyraźnie zapisano iż: Realizacja tego wymagania nie będzie mogła korzystać z zamówionej puli Roboczodni.</p>	

Identyfikator	R-APP-002
<p>Na żądanie Zamawiającego Wykonawca przeprowadzi analizę wymagań funkcjonalnych i poza funkcjonalnych określonych przez Zamawiającego. Przedstawi propozycję rozbudowy (realizacji i implementacji zmian w systemie PLI CBD) podając ilość Roboczodni pracy z tym związanej. (Roboczodni będą uszczuplały pulę Roboczodni).</p>	

Identyfikator	R-APP-003
<p>Po uzyskaniu akceptacji ilości Roboczodni ze strony Zamawiającego dla propozycji rozbudowy Systemu PLI CBD, Wykonawca przygotowuje rozwiązanie techniczne i dokona jego testów przy współudziale Zamawiającego. Zamawiający zastrzega sobie możliwość zaproszenia do testów stron trzecich.</p>	

Identyfikator	R-APP-004
---------------	-----------

Po akceptacji ze strony Zamawiającego rozwiązania w środowisku testowym, Wykonawca wdroży funkcjonalności do eksploatacji. Wykonawca przygotuje aktualizację dokumentacji technicznej oraz instrukcji użytkowych. Po wdrożeniu zmian Wykonawca przeprowadzi szkolenia dla obsługi PLI CBD. Ponadto Wykonawca zobowiązany będzie do usunięcia wszystkich wad wprowadzonych zmian Systemu PLI CBD zarówno na etapie ich wdrażania, jak i późniejszej eksploatacji Systemu PLI CBD. Usuwanie wad nie będzie uszczuplało puli roboczodni.

Identyfikator	R-APP-005
----------------------	------------------

Wprowadzenie możliwości interwencyjnego zamykania każdej sprawy NP przez Obsługę PLI CBD. Utworzenie funkcjonalności w module NPAdministrationWeb, w której po wpisaniu numeru sprawy i akceptacji, sprawa zostanie zamknięta. Do Dawcy i Biorcy zostanie przesłany stosowny komunikat informujący Exx.

Identyfikator	R-APP-006
----------------------	------------------

Po zakończeniu umowy wykonawca jest zobowiązany do zapewnienia wsparcia w wyjaśnianiu ewentualnych rozbieżności/braków w kodzie aplikacji wykrytych przez nowego wykonawcę. Wsparcie ma być zapewnione od momentu podpisania umowy z nowym wykonawcą do czasu potwierdzenia przez nowego wykonawcę zgodności kodu.

Identyfikator	R-APP-007
----------------------	------------------

W ramach realizacji wymagania Wykonawca dokona wdrożenia (na środowisko produkcyjne) modyfikacji poziomów przechowywania danych o zakresach numeracji oraz numerach przeniesionych w systemie PLI CBD.
Zamawiający udostępni Wykonawcy posiadaną dokumentację i kody źródłowe funkcjonalności działającej na środowisku testowym.
Realizacja tego wymagania nie będzie mogła korzystać z zamówionej puli Roboczodni.