Załącznik nr …. do wniosku

OPIS PRZEDMIOTU ZAMÓWIENIA

Sprzęt i oprogramowanie dla Warstwy Regionalnej w projekcie Zachodniopomorskie e-Zdrowie.

Spis treści

SPIS TREŚCI 2

Rozdział I. Założenia początkowe oraz wymagania ogólne

I.1 Wprowadzenie

Zamówienie realizowane jest w ramach projektu „Zachodniopomorskie e-Zdrowie" współfinansowanego środkami Unii Europejskiej w ramach Regionalnego Programu Operacyjnego Województwa Zachodniopomorskiego na lata 2014-2020 Oś Priorytetowa 9 Infrastruktura publiczna, Działanie 9.10 Wsparcie rozwoju e-usług publicznych (e-Zdrowie).
Przedmiotowe postępowanie dotyczy realizacji Platformy Regionalnej w Urzędzie Marszałkowskim Województwa Zachodniopomorskiego będącego jednocześnie Zamawiającym i Liderem Projektu.

I.2 Integracja z centralnym systemem e-zdrowie

1. Regionalny System Informatyczny (RSI) musi zapewniać integrację funkcjonalną z systemem teleinformatycznym, o którym mowa w art. 7 ust. 1 ustawy o systemie informacji w ochronie zdrowia (Dz.U. 2020, poz. 702 z późn. zm.), co najmniej w zakresie opisanym w dokumentach opublikowanych przez Centrum e-Zdrowia (dotychczas CSIOZ), tj.:
   1) „Opis usług biznesowych Systemu P1 wykorzystywanych w systemach usługodawców",
   2) „Opis funkcjonalny Systemu P1 z perspektywy integracji systemów zewnętrznych"

   oraz dokumentacją:

   3) „Minimalne wymagania dla systemów usługodawców (https://www.gov.pl/web/zdrowie/minimalne-wymagania-dla-systemow-uslugodawcow)
   4) Dokumentacja integracyjna Systemu P1 w zakresie obsługi EDM,
   5) Dokumentacja integracyjna Systemu P1 w zakresie obsługi zgód pacjenta
2. W zakresie integracji i komplementarności z centralnymi systemami e-zdrowie, na Wykonawcy będzie spoczywał obowiązek dostosowania zaoferowanego rozwiązania do wymagań ujętych w dokumentach publikowanych poprzez Centrum e-Zdrowia, w tym w szczególności do wszelkiej dokumentacji integracyjnej.
3. Dokumenty, o których mowa powyżej są dostępne na stronie internetowej Centrum e-Zdrowia, pod adresem: http://cez.gov.pl oraz http://ezdrowie.gov.pl.
4. W zakresie integralności zaoferowanego Regionalnego Systemu Informatycznego Wykonawca powinien uwzględnić i wdrożyć poniższe wytyczne i założenia w przypadku obowiązywania wymogu:
   1) Dostępność Systemu P1 dla odpowiednio zarejestrowanych w Centrum e-Zdrowia systemów usługodawców i systemów regionalnych wyłącznie poprzez standardowe interfejsy Web Services. Wymagane jest dwustronne uwierzytelnianie systemów nawiązujących komunikację, a także podpisywanie komunikatów certyfikatem dostarczanym bądź wskazanym przez Centrum e-Zdrowia.
   2) Przesyłanie komunikatów do P1 podpisanych elektronicznie przez system komunikujący się z Systemem P1 certyfikatem wydanym przy zakładaniu konta usługodawcy (rejestrowaniu

systemu). Wymagania w zakresie rodzaju stosowanego certyfikatu mogą ulec zmianie w wyniku wejścia w życie Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (rozporządzenie eIDAS) oraz wprowadzenia centralnych rozwiązań w zakresie uwierzytelniania użytkowników w obszarze e-zdrowie.

3) Zgoda pacjenta na udostępnienie jego dokumentacji medycznej – funkcjonalność ta jest wymagana i powinna być zgodna z modelem dokumentu zgody oraz modelami interfejsów pozwalających na wnioskowanie o zgodę, które zostaną opublikowane przez Centrum e-Zdrowia.

4) Wymiana Elektronicznej Dokumentacji Medycznej (dalej: EDM) – funkcjonalność ta jest wymagana i powinna być zgodna z modelem wniosku i dokumentu udostępnienia oraz modelami interfejsów, które zostaną opublikowane przez Centrum e-Zdrowia.

5. Jednocześnie, zaoferowany Regionalny System Informatyczny powinien spełniać następujące założenia funkcjonalne:

1) Regionalny System Informatyczny musi uwzględniać funkcjonalności dotyczące prowadzenia repozytorium EDM (w zakresie Document Repository) oraz uwzględniać rozwiązania zapewniające wymianę EDM pomiędzy repozytorium, a Platformą P1.

2) Repozytorium EDM musi realizować, co najmniej usługę przyjmowania, archiwizacji i udostępniania EDM zgodnej z HL7 CDA, a w przypadku repozytoriów badań obrazowych, przyjmowania, archiwizacji i udostępniania obiektów DICOM.

I.3 Akty prawne

Dostarczone rozwiązania teleinformatyczne, ze szczególnym uwzględnieniem dostarczanego i wdrażanego Oprogramowania, muszą być zgodne z powszechnie obowiązującymi przepisami prawa polskiego i europejskiego. Oprogramowanie musi pozwalać na gromadzenie, przetwarzanie i analizowanie danych i informacji w obszarach objętych wdrożeniem, na bazie tych danych musi umożliwiać wytwarzanie prawidłowej, kompletnej, ujętej w obowiązujących przepisach prawa dokumentacji (dokumenty, raporty, wykazy, oświadczenia, zaświadczenia itp.).

I.4 Ogólny opis przedmiotu zamówienia

1. Przedmiot zamówienia obejmuje:

a) Modernizacja sieci teleinformatycznej w zakresie:

POZ. OPZ	OPIS	ILOŚĆ
ROZDZIAŁ II.1	**INFRASTRUKTURA SIECIOWA**	
II.1.1	UTM	2
II.1.2	Przełącznik serwerowy LAN	4

II.1.3	Przełącznik zasobowy - SAN	4
II.1.4	Szafa 42U z wyposażeniem	2
II.1.5	Konsola KVM+KMM	2

b) Infrastruktura serwerowa w zakresie:

POZ. OPZ	OPIS	ILOŚĆ
ROZDZIAŁ II.2	**INFRASTRUKTURA SERWEROWA**	
II.2.1	Serwer lokalizacja nr 1	3
II.2.2	Serwer lokalizacja nr 2	3
II.2.3	Macierz dyskowa	2
II.2.4	Biblioteka taśmowa	1
II.2.5	Serwer kopii bezpieczeństwa	1
II.2.6	Deduplikator	1

c) Oprogramowanie systemowe i narzędziowe w zakresie:

POZ. OPZ	OPIS	ILOŚĆ
ROZDZIAŁ II.3	**OPROGRAMOWANIE SYSTEMOWE I NARZĘDZIOWE**	
II.3.1	Serwerowy system operacyjny	12
II.3.2	Oprogramowanie wirtualizacyjne	1
II.3.3	Oprogramowanie backupowe	1
II.3.4	System ochrony aplikacji webowych oraz XML	1

d) dostawę i wdrożenie Regionalnego Systemu Informatycznego RSI:

POZ. OPZ	OPIS
ROZDZIAŁ II.4	**REGIONALNY SYSTEM INFORMATYCZNY**
II.4	Dostawa i wdrożenie: - Regionalne Repozytorium EDM - Portal Projektu ZeZ

2. Wszystkie dostarczane Produkty (rozumiane jako elementarny efekt działań/prac/dostaw objętych całym zakresem przedmiotu zamówienia wykonywanych przez Wykonawcę podczas realizacji Umowy w poszczególnych Etapach) oraz Komponenty (rozumiane jako integralna część dostawy i wdrożenia przedmiotu zamówienia, składający się przynajmniej z jednego Produktu lub wielu Produktów powiązanych ze sobą merytorycznie) podlegają usługom projektowania, dostaw, instalacji, konfiguracji i wdrożenia.

3. Usługi projektowania, instalacji, konfiguracji i wdrożenia Wykonawca musi przeprowadzić zgodnie z postanowieniami niniejszego OPZ w uzgodnieniu z Zamawiającym, zgodnie z obowiązującymi przepisami, zasadami wykonywania projektów teleinformatycznych oraz najlepszymi praktykami w ich realizacji.
4. Wykonawca jest zobowiązany do realizacji Przedmiotu Zamówienia zgodnie z zasadami i wytycznymi Zamawiającego, zapisami OPZ oraz Umowy.
5. Ilekroć w niniejszym OPZ Zamawiający użył w opisie oznaczeń norm, aprobat, specyfikacji technicznych i systemów odniesienia, o których mowa w art. 101 ust. 1-3 ustawy Pzp należy je rozumieć jako przykładowe. Zamawiający zgodnie z art. 101 ust. 4 ustawy Pzp dopuszcza rozwiązania równoważne opisywanym w treści SWZ. Jeżeli zapisy zawarte w OPZ wskazywałyby w odniesieniu do rozwiązań, materiałów lub urządzeń znaki towarowe lub pochodzenie Zamawiający, zgodnie z art. 101 ust. 4 ustawy Pzp dopuszcza składanie ofert na rozwiązania równoważne dla których Zamawiający w każdym z przypadków przedstawia stosowny opis równoważności. Wszelkie „produkty" pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, jakim musi odpowiadać produkt, aby spełnić wymagania stawiane przez Zamawiającego stanowią wyłącznie wzorzec jakościowy przedmiotu zamówienia. Poprzez zapis dot. minimalnych wymagań parametrów jakościowych Zamawiający rozumie wymagania materiałów, sprzętu i urządzeń zawarte w ogólnie dostępnych źródłach, katalogach, stronach internetowych producentów. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w+ stosunku do określonego rozwiązania. Tak więc posługiwanie się nazwami producentów /produktów/ ma wyłącznie charakter przykładowy.
6. Wykonawca musi dostarczyć wszelkie urządzenia i elementy, które są niezbędne do prawidłowego funkcjonowania całości. W przypadku, gdy w trakcie realizacji Przedmiotu Zamówienia okaże się, że brakuje jakiegokolwiek urządzenia lub elementu, którego brak spowoduje nieprawidłowe funkcjonowanie całości Przedmiotu Zamówienia, Wykonawca dostarczy je na własny koszt.
7. Wszelkie dostarczane urządzenia:
   1) muszą być fabrycznie nowe, pochodzić z autoryzowanego kanału sprzedaży producenta oraz muszą reprezentować model bieżącej linii produktowej. Nie dopuszcza się urządzeń odnawianych, demonstracyjnych lub powystawowych,
   2) nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta,
   3) elementy, z których zbudowane są urządzenia muszą być produktami producenta urządzeń lub muszą być przez niego certyfikowane oraz w całości muszą być objęte gwarancją producenta,

4) urządzenia i ich komponenty muszą być oznakowane w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta,

5) urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach producenta,

6) do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w języku polskim lub angielskim, w formie papierowej lub elektronicznej.

I.5 Termin realizacji Przedmiotu Zamówienia

Zamawiający wymaga wykonania przedmiotu zamówienia w terminie 9 miesięcy od daty zawarcia umowy.

I.6 Powiązania między OPZ a Modelem Realizacyjnym

1. Zakres, kształt oraz funkcjonalności poszczególnych usług elektronicznych w projekcie „Zachodniopomorskie e-Zdrowie" określone zostały w Modelu realizacyjnym – załącznik nr ..... do SWZ.
2. W przypadku różnic w zakresie e-usług oraz funkcjonalności Projektu ZeZ między niniejszym Opisem Przedmiotu Zamówienia a Modelem realizacyjnym nadrzędne są wymagania zawarte w niniejszym Opisie Przedmiotu Zamówienia oraz Umowie.

I.7 Organizacja wdrożenia

I.7.1 Założenia podstawowe

1. Przedmiot Zamówienia będzie realizowany w oparciu o zdefiniowany uprzednio przez Wykonawcę i zaakceptowany Harmonogram wdrożenia, który powinien być uzgodniony i zaakceptowany przez Zamawiającego oraz odpowiednio utrzymywany w toku realizacji Przedmiotu Zamówienia. Wykonawca musi przedstawić Harmonogram wdrożenia w terminie 14 dni od daty podpisania umowy.
2. Wykonawca w Harmonogramie wdrożenia musi uwzględnić w szczególności podział na zadania takie jak projektowanie, dostawy, usługi instalacji/konfiguracji, testowanie, wdrożenie i odbiory.
3. Wykonawca umożliwi Zamawiającemu udział we wszystkich pracach realizowanych przez Wykonawcę w ramach realizacji Przedmiotu Zamówienia (m.in. w czasie projektowania, dostawach, instalacji/budowie, konfiguracji i wdrożeniu i testowaniu).
4. Wykonawca zobowiązany jest do udziału w cyklicznych naradach przeglądu prac w siedzibie Zamawiającego. Dopuszcza się narady prowadzone w trybie zdalnym z wykorzystaniem narzędzi komunikacji elektronicznej, które zapewni Wykonawca. Zamawiający przewiduje częstotliwość narad maksymalnie 1 raz w miesiącu, narad zdalnych maksymalnie 3 razy w miesiącu, chyba że nadzwyczajna sytuacja w realizacji przedmiotu umowy wymagała będzie częstszych spotkań w siedzibie lub odbywanych zdalnie.

5. Wykonawca zobowiązany jest przeprowadzić dostawy Przedmiotu Zamówienia w dokładnych terminach i godzinach uzgodnionych z Zamawiającym.
6. W przypadku dostarczania Infrastruktury Serwerowej oraz Sieciowej musi być ona oznakowana w taki sposób, aby możliwa była identyfikacja systemowa zarówno produktu jak i producenta, pochodzić z oficjalnych kanałów dystrybucji producentów i dostarczona w oryginalnych opakowaniach fabrycznych.
7. Wdrożenie należy rozumieć jako szereg uporządkowanych i zorganizowanych działań mających na celu wykonanie Przedmiotu Zamówienia.
8. Wdrożenie będzie realizowane w ramach powołanych do tego celu struktur organizacyjnych po stronie Wykonawcy.
9. W ramach wdrożenia Wykonawca musi przygotować informacje na temat struktury organizacyjnej Zespołu Wykonawcy zajmującej się realizacją przedmiotu zamówienia, w ramach której muszą zostać powołane minimum następujące role:
    1) Kierownik Projektu ze strony Wykonawcy,
    2) Zespół Wdrożeniowy ze strony Wykonawcy.
10. Wdrożenie, z zastrzeżeniami wskazanymi poniżej muszą realizować osoby wymienione w ofercie Wykonawcy, przy czym:
    1) Osoby Zespołu Wykonawcy muszą być dyspozycyjne w trakcie wykonywania prac,
    2) Wykonawca musi przekazać Zamawiającemu wykaz numerów telefonów kontaktowych do kluczowych osób biorących udział w realizacji Przedmiotu Zamówienia po stronie Wykonawcy.
11. Wykonawca musi zorganizować prace tak, aby w maksymalnym stopniu nie zakłócać ciągłości funkcjonowania prac u Zamawiającego.
12. Obiekty podlegające inwestycji są użytkowane w trybie ciągłym w czasie godzin pracy przez cały okres wykonywania przedmiotu zamówienia, co może powodować utrudnienia w miejscu prowadzenia prac. Nie ma możliwości całkowitego wyłączenia i zamknięcia w/w obiektów lub ich części na czas realizacji przedmiotu zamówienia. Poszczególne prace będą realizowane etapowo, tak aby zachować ciągłość świadczenia usług przez Zamawiającego.
13. Wykonawca musi uwzględnić, że wszystkie prace będą wykonywane w użytkowanych obiektach przy ruchu pracowników Zamawiającego, tzn. organizacja prac musi przede wszystkim zapewniać bezpieczeństwo przebywających w obiekcie pracowników Zamawiającego.

I.7.2 Przygotowanie Dokumentacji

1. W ramach realizowanych prac Wykonawca musi opracować dla Zamawiającego Dokumentację Przedmiotu Zamówienia (zwaną dalej Dokumentacją), która składa się z niżej wymieniownych zakresów:
    1) Harmonogram Wdrożenia,
    2) Dokumentacja Analizy Przedwdrożeniowej (DAP),

3) Dokumentacja Powykonawcza.

2. Dokumentacja powyższa musi zawierać bazowe zapisy opisujące budowane rozwiązania, procesy oraz sposób organizacji prac i wdrożenia. Na podstawie zapisów w Dokumentacji będą prowadzone i odbierane poszczególne etapy realizowane w ramach przedmiotu zamówienia. Dokumenty te wraz ze SWZ z załącznikami będą stanowiły podstawę do weryfikacji wdrożenia w trakcie odbiorów.
3. Dokumentacja podlega uzgadnianiu i akceptacji Zamawiającego. Akceptacja Harmonogramu wdrożenia i DAP warunkuje rozpoczęcie prac Wykonawcy.
4. Dokumentacja Analizy Przedwdrożeniowej DAP wraz z Harmonogramem wdrożenia muszą być opracowane w oparciu o wymagania określone w niniejszym OPZ.

I.7.3 Harmonogram wdrożenia

Wykonawca zobowiązany jest opracować na podstawie SWZ oraz OPZ szczegółowy Harmonogram wdrożenia. Harmonogram należy przedstawić Zamawiającemu w terminie do 14 dni od daty zawarcia Umowy.

I.7.4 Analiza Przedwdrożeniowa

1. Analiza Przedwdrożeniowa obejmuje czynności do wykonania przez Wykonawcę mające na celu analizę środowiska biznesowego i informatycznego Zamawiającego. W wyniku przeprowadzenia Analizy Przedwdrożeniowej Wykonawca przedstawi Zamawiającemu Dokumentację Analizy Przedwdrożeniowej (zwana dalej DAP), na podstawie której organizacyjnie i technicznie będzie realizowany przedmiot zamówienia. DAP będzie podlegała uzgodnieniu i akceptacji Zamawiającego.
2. DAP musi zawierać w szczególności:

ZAWAROŚĆ DOKUMENTACJI ANALIZY PRZEDWDROŻENIOWEJ DAP
1. Wymagane dane w zakresie RSI
1) wykaz oraz szczegółowy opis i harmonogram budowy RSI i e-usług,
2) architekturę RSI i e-usług,
3) przygotowanie planu instalacji Infrastruktury serwerowej z uwzględnieniem rozmieszczenia sprzętu w lokalizacjach Zamawiającego,
4) przygotowanie planu instalacji macierzy dyskowych,
5) jednoznacznie określone założenia integracji z innymi systemami informatycznymi, które posiada Zamawiający,
6) szczegółową specyfikację oprogramowania objętego zakresem umowy,
7) wykaz oraz szczegółowy opis i harmonogram niezbędnych prac konfiguracyjnych,
8) ustawienia konfiguracyjne urządzeń i oprogramowania wchodzących w skład RSI,
9) propozycje scenariuszy testowych uwzględniających zakres czynności operacyjnych, które należy wykonać w celu potwierdzenia, że wskazane wymagane funkcjonalności zostały prawidłowo skonfigurowane i działają zgodnie z opisami procesów,

10) harmonogram instruktażu personelu oraz administratorów RSI.
Wymagane dane ZARZĄDCZE:
plan i sposób komunikacji Stron.
Wymagane dane w zakresie INFRASTRUKTURY SERWEROWEJ
1) podział Przedmiotu Zamówienia na Produkty, a następnie ich pogrupowanie w Komponenty,
2) analizę wymagań Przedmiotu Zamówienia zawierającą opis sposobu realizacji wymagań, sposób testowania i odbioru,
3) karty katalogowe urządzeń potwierdzające spełnienie wymagań,
4) plan dostaw,
5) opis instalacji i wdrożenia oprogramowania wdrażanego wraz z Infrastrukturą serwerową,
6) opis modernizacji i budowy Infrastruktury serwerowej,
7) lista Komponentów, które będę podlegały osobnym odbiorom – jeżeli dotyczy,
8) szczegółowy zakres i zawartość pozostałej Dokumentacji.
Wymagane dane w zakresie INFRASTRUKTURA SIECIOWA
1) podział Przedmiotu Zamówienia na Produkty, a następnie ich pogrupowanie w Komponenty,
2) analizę wymagań Przedmiotu Zamówienia zawierającą opis sposobu realizacji wymagań, sposób testowania i odbioru,
3) karty katalogowe urządzeń potwierdzające spełnienie wymagań,
4) dokumentację i plan dostaw,
5) Plan, opis instalacji i wdrożenia oprogramowania wdrażanego wraz z aktywną Infrastrukturą sieciową,
6) listę Komponentów, które będę podlegały osobnym odbiorom – jeżeli dotyczy,
7) szczegółowe uzgodnienia Stron Umowy dotyczące zakresu i sposobu integracji dostarczanych rozwiązań z istniejącą infrastrukturą u Zamawiającego ,
8) zakres prac realizowanych przez podwykonawców,
9) szczegółowy zakres i zawartość pozostałej Dokumentacji.

I.7.5 Dokumentacja Powykonawcza

1. Warunkiem dokonania Odbioru Końcowego jest dostarczenie przez Wykonawcę Dokumentacji Powykonawczej obejmującej dokumentację użytkową, techniczną i eksploatacyjną. Dokumentacja Powykonawcza musi być dostarczona w języku polskim, w wersji elektronicznej w formacie edytowalnym oraz w co najmniej jednym egzemplarzu papierowym.
2. W dokumentacji muszą być zawarte opisy wszelkich cech, właściwości i funkcjonalności pozwalających na poprawną z punktu widzenia technicznego eksploatację rozwiązań.
3. W szczególności dokumentacja ta musi zawierać:
   1) **Wymogi ogólne:**
      a) pełną charakterystykę licencjonowania wszystkich elementów aplikacji i środowiska,
      b) opis architektury technicznej:
         - wyszczególnienie oraz opis powiązań wszystkich komponentów sprzętowych, systemowych i aplikacyjnych występujących lub wymaganych do poprawnej

pracy aplikacji zgodnie z wymaganiami wydajności, funkcjonalności i bezpieczeństwa (minimalny, maksymalny, rekomendowany),
- dokładne określenie wykorzystywanych i dopuszczalnych wersji dla komponentów innych dostawców,

c) konfiguracja musi obejmować wszystkie wdrożone urządzenia, zainstalowane w ramach budowy systemu IT,
d) przykładowy zestaw wymaganych danych konfiguracyjnych obejmuje:
- serwery – parametry sprzętowe (procesor, pamięć, dyski, karty sieciowe, zasilanie, itp.),
- sieć (adresacja IP, itp.),
- podsystem dyskowy (punkty montowania/litery dysków, wolumeny logiczne, grupy wolumenowe, zasoby dyskowe, RAID, itp.),
- system operacyjny (parametry jądra, moduły, usługi, stos TCP/IP, itp.),
- klaster (węzły fizyczne, paczki klastrowe, kolejność przełączania, itp.),
- listę zainstalowanego oprogramowania, itp.,
- macierze – parametry sprzętowe (cache, półki dyskowe, dyski, karty/porty fibre channel, itp.), grupy dyskowe, zasoby dyskowe, maskowanie, kopie biznesowe, replikacja, itp.,
- infrastruktura sieciowa – parametry sprzętowe (porty fibre channel, aktywne licencje, itp.), fabric, zonning, aliasy, itp.,

e) opis architektury logicznej:
- schemat i opis powiązań logicznych poszczególnych komponentów i ich role w architekturze,

f) mapę i opis Interface'ów.
- interfejsy muszą zawierać szczegółowy opis techniczny, w szczególności zawierać informację o: typie interfejsu, wykorzystywanych protokołach, portach sieciowych, strukturze interfejsu, itp. oraz o zakresie wymiany danych i sposobu kontroli prawidłowości działania,

g) opis wymagań sprzętowych, systemowych, sieciowych itp.
- wymagania dla poszczególnych komponentów architektury, odniesienia do oczekiwanych wymagań wydajnościowych, funkcjonalnych i bezpieczeństwa (minimalny, maksymalny, rekomendowany),

h) procedury lub instrukcje instalacji, reinstalacji, deinstalacji oraz aktualizacji.
- szczegółowy opis postępowania w przypadku tworzenia lub zmian w środowisku; jeśli wykorzystywane są procedury innych dostawców dla standardowych komponentów (np. baz danych) wystarczy wskazać w dokumentacji szczegółowe odniesienie do procedur standardowych właściwych dla tych komponentów,

i) dokumentację administracyjną związaną z poprawną eksploatacją:
- opis (w postaci procedur lub instrukcji) wszystkich rutynowych czynności administracyjnych dla aplikacji i systemu informatycznego (dziennych, tygodniowych, miesięcznych itp.) oraz działań pozwalających na utrzymanie wymaganej dostępności, wydajności i bezpieczeństwa,

j) dokumenty z testów:
- plan testów, scenariusze testowe i protokoły z testów akceptacyjnych, wydajnościowych, testów operacji administratora technicznego, testów

bezpieczeństwa w tym ciągłości działania (przełączanie, odtwarzanie, weryfikacja poprawności), testów funkcjonalnych oraz testów procedur eksploatacyjnych.

k) dokumentację wdrożeniową:
   - dokumentacja powdrożeniowa: zawiera szczegółowy opis wykonanych czynności instalacyjnych oraz konfiguracyjnych wszystkich komponentów systemu,
   - dokumentacja parametryzacji: wyszczególnienie wartości wszystkich ustawionych parametrów użytkowych zarówno samej aplikacji jak i pozostałych komponentów systemu, parametry systemu operacyjnego oraz parametry sprzętu, w tym konfiguracji środowiska produkcyjnego (serwery baz danych, serwery aplikacji, inne zastosowane),
   - dokumentacja uruchomieniowa: opisuje wszystkie istotne kroki (czynności) wykonane w celu pierwszego uruchomienia aplikacji/systemu, w tym opis migracji/konwersji danych, testy uruchomieniowe,
   - dokumentacja pilotażowa: jeśli był stosowany w trakcie wdrożenia pilotaż jako element stabilizacji i testów,

l) wersjonowanie:
   - opis zasad wersjonowania i sposobu patchowania aplikacji,

m) zalecenia:
   - opis zasad i zaleceń strojenia aplikacji,

n) instrukcje obsługi i instrukcje użytkowania dla wersji dostarczonego oprogramowania z podziałem na poszczególne moduły,

o) w zakresie obszarów administratora dokumentacja musi zawierać dodatkowo co najmniej:
   - opis podstawowych ról użytkowników i zasad ich kreowania,
   - opis zarządzania uprawnieniami użytkownika i tworzenia profili,
   - lista dostępnych uprawnień użytkownika wraz z opisem efektu w zakresie dostępu do danych w RSI lub/i e-usług,
   - opis zarządzania autoryzacją i autentykacją użytkowników,

p) wkład do Polityki bezpieczeństwa w zakresie wdrożonego Systemu oraz Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych opracowany zgodnie z wymaganiami określonymi w Rozporządzeniu 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). Wkład do Polityki Bezpieczeństwa musi zawierać w szczególności:
   - wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
   - opis struktury zbiorów danych wskazującej zawartość poszczególnych pól informacyjnych i powiązań między nimi,
   - informacje o sposobie przepływu danych pomiędzy poszczególnymi systemami,
   - opis środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

2) Wymogi szczegółowe:

a) opis aplikacji i konfiguracji aplikacji/systemu:

- opis musi obejmować ogół oprogramowania wdrożonego, zainstalowanego w ramach budowy systemu IT,
- opis musi zawierać opis systemu lub systemów informatycznych, zawierający wykaz programów, procedur lub funkcji, w zależności od struktury oprogramowania, wraz z opisem algorytmów i parametrów oraz programowych zasad ochrony danych, w tym w szczególności metod zabezpieczania dostępu do danych i systemu ich przetwarzania, sposobu komunikacji pomiędzy systemami, zakresu wymienianych danych i sposobu ich szyfrowania,
- przykładowy zestaw wymaganych danych konfiguracyjnych obejmuje: wersję oprogramowania, narzędzia, użytkowników i grupy systemowe, katalog instalacyjny, położenie plików konfiguracyjnych, pierwotne parametry konfiguracyjne i zmodyfikowane w procesie instalacji, położenie plików logów, położenie i opis innych kluczowych plików i katalogów, parametry instancji, itp.,
- konfiguracja musi obejmować wersję aplikacji, pełen zestaw parametrów konfiguracyjnych aplikacji wraz z opisem użycia, katalogi instalacyjne, położenie plików konfiguracyjnych, położenie plików logów, położenie i opis innych kluczowych plików i katalogów, itp.,

b) procedury tworzenia środowisk pomocniczych:
- zasady i procedury tworzenia środowisk (testowych, rozwojowych, raportowych) oraz metod klonowania i anonimizacji (depersonifikacji) danych przenoszonych pomiędzy środowiskami,

c) procedury eksploatacji:
- procedury odtworzenia systemów i środowiska informatycznego danego Zamawiającego po katastrofie (Disaster Recovery),
- procedury muszą opisywać kolejne kroki pozwalające na bezpieczne zatrzymanie/uruchomienie elementu infrastruktury hardware'owej oraz aplikacji i elementów infrastruktury software'owej, lub całego środowiska sprzętowo-software'owego.
- dokumenty muszą obejmować również procedury i instrukcje instalacji krok po kroku środowiska produkcyjnego „od podstaw" na: środowisku fizycznych hostów danego Zamawiającego rozpoczynając od dostarczonego wirtualizatora oraz standardowym zastosowanym systemie operacyjnym dla poszczególnych dostarczonych systemów informatycznych.
- w szczególności dokumentacja musi zawierać procedury tworzenia/odtwarzania kopii bezpieczeństwa operacyjnego i kopii zapasowych oraz odtwarzania/kreowania z kopii wszystkich komponentów aplikacji i środowiska (bazy danych, komponenty serwera aplikacji, klienta itp.),

d) Procedury backupowe:
- zalecany tryb backupu aplikacji i elementów infrastruktury software'owej oraz zakres danych podlegających backupowi. Procedury odtworzeniowe muszą w szczególności opisywać sposób odtworzenia funkcjonalności aplikacji i elementów infrastruktury software'owej w przypadku błędu lub awarii.

I.7.6 Odbiór Etapu/Dokumentacji/Końcowy

1. Odbiory Etapów/Dokumentacji będą się odbywać po zakończeniu określonych prac danego Etapu/Dokumentacji.
2. Odbiór końcowy Przedmiotu Zamówienia ma na celu potwierdzenie wykonania wszystkich zadań wynikających z Umowy, w tym odebrania wszystkich Komponentów i Etapów oraz dostarczenia wymaganej zamówieniem Dokumentacji.
3. Odbiory będą odbywać się zgodnie z zapisami w Umowie stanowiącej załącznik nr X do SWZ.

I.7.7 Dostawa i instalacja oprogramowania standardowego

1. Oprogramowanie standardowe rozumiane jako oprogramowanie dostarczone i zainstalowane na Infrastrukturze serwerowej oraz sieciowej posiadanej przez Zamawiającego lub dostarczanym zgodnie z Umową stanowiącą załącznik nr X do SWZ oraz w istniejących systemach informatycznych zgodnie z wymaganiami niniejszego Opisu Przedmiotu Zamówienia w taki sposób, aby zapewnić prawidłowe funkcjonowanie Oprogramowania aplikacyjnego, sprzętu oraz istniejących systemów informatycznych na wszystkich stanowiskach pracy (stanowiska komputerowe) Zamawiającego.
2. Dostawa i instalacja zostaną wykonane w lokalizacjach zgodnych z instalacją urządzeń u Zamawiającego i zgodnie z Harmonogramem wdrożenia.
3. Oprogramowanie standardowe musi zostać skonfigurowane tak, aby działało poprawnie zgodnie z jego przeznaczeniem i architekturą Systemu oraz zapewniało prawidłową pracę Oprogramowania aplikacyjnego.

I.7.8 Dostawa, instalacja, konfiguracja i wdrożenie Oprogramowania aplikacyjnego

1. Zadanie dostawy, instalacji, konfiguracji i wdrożenia Oprogramowania aplikacyjnego obejmuje:

POZ. OPZ	OPIS
ROZDZIAŁ II.4	**REGIONALNY SYSTEM INFORMATYCZNY**
II.4	Dostawa i wdrożenie: - Regionalne Repozytorium EDM - Portal Projektu ZeZ

2. Dostawa i instalacja mają być wykonane w wyznaczonych lokalizacjach Zamawiającego.
3. Po zakończeniu prac instalacyjnych Oprogramowanie musi zostać skonfigurowane i wdrożone w sposób kompleksowy tak, aby oferowało wszystkie funkcjonalności opisane w SWZ oraz zgodnie z Dokumentacją i wskazanymi przez Zamawiającego wytycznymi na etapie analizy przedwdrożeniowej oraz oczekiwaniami konfiguracyjnymi samego procesu wdrażania (w zakresie opisanych w OPZ wymagań funkcjonalnych).
4. Oprogramowanie aplikacyjne musi zostać zainstalowane przez Wykonawcę w szczególności z wykorzystaniem Sprzętu dostarczanego przez Wykonawcę i w środowiskach informatycznych

Zamawiającego. Oprogramowanie aplikacyjne musi zostać zainstalowane i skonfigurowane w sposób kompleksowy na wszystkich stanowiskach komputerowych Zamawiającego.

5. Zamawiający na potrzeby realizacji przedmiotu zamówienia przewidział infrastrukturę serwerową i oprogramowanie o parametrach wskazanych w rozdziale II niniejszego OPZ.

I.7.9 Testy

1. W ramach postepowania muszą zostać przeprowadzone wszystkie testy opisane w Dokumentacji. Celem testów jest weryfikacja przez Zamawiającego czy wszystkie prace wykonane w trakcie realizacji Przedmiotu Zamówienia zostały wykonane prawidłowo i zgodnie z założeniami funkcjonalnymi i jakościowymi. Testy będą przeprowadzane przez Wykonawcę przy współudziale Zamawiającego jak i wskazanych przez Zamawiającego osób i podmiotów zewnętrznych.
2. Pozytywne zakończenie testów wraz z usunięciem wskazanych Wad jest niezbędne, aby dla poszczególnych Komponentów oraz całego Przedmiotu Zamówienia dokonać odbiorów w ramach poszczególnych Etapów i Odbioru końcowego.
3. Zamawiający ma prawo do weryfikacji należytego wykonania Umowy dowolną metodą, w tym także z wykorzystaniem opinii zewnętrznego audytora. W szczególności uzgodnienie określonych scenariuszy testowych nie wyklucza prawa do weryfikacji prac innymi testami i scenariuszami.
4. W przypadku zidentyfikowania Błędów lub Wad Wykonawca jest zobowiązany do ich poprawy przed odbiorem Końcowym Przedmiotu Zamówienia.

I.7.10 Dodatkowe zobowiązania Wykonawcy

1. Wykonanie Przedmiotu Zamówienia z efektywnością oraz zgodnie z praktyką i wiedzą zawodową.
2. Dokonanie z Zamawiającym wszelkich koniecznych ustaleń mogących wpływać na zakres i sposób realizacji Przedmiotu Zamówienia oraz ciągła współpraca z Zamawiającymi na każdym etapie realizacji.
3. Stosowanie się do wytycznych i polityk bezpieczeństwa informacji obowiązujących u Zamawiającego.
4. Udzielanie na każde żądanie Zamawiającego pełnej informacji na temat stanu realizacji Przedmiotu Zamówienia.
5. Współdziałanie z osobami wskazanymi przez Zamawiającego.

Rozdział II. Szczegółowy opis przedmiotu zamówienia

1. Opis rozwiązania

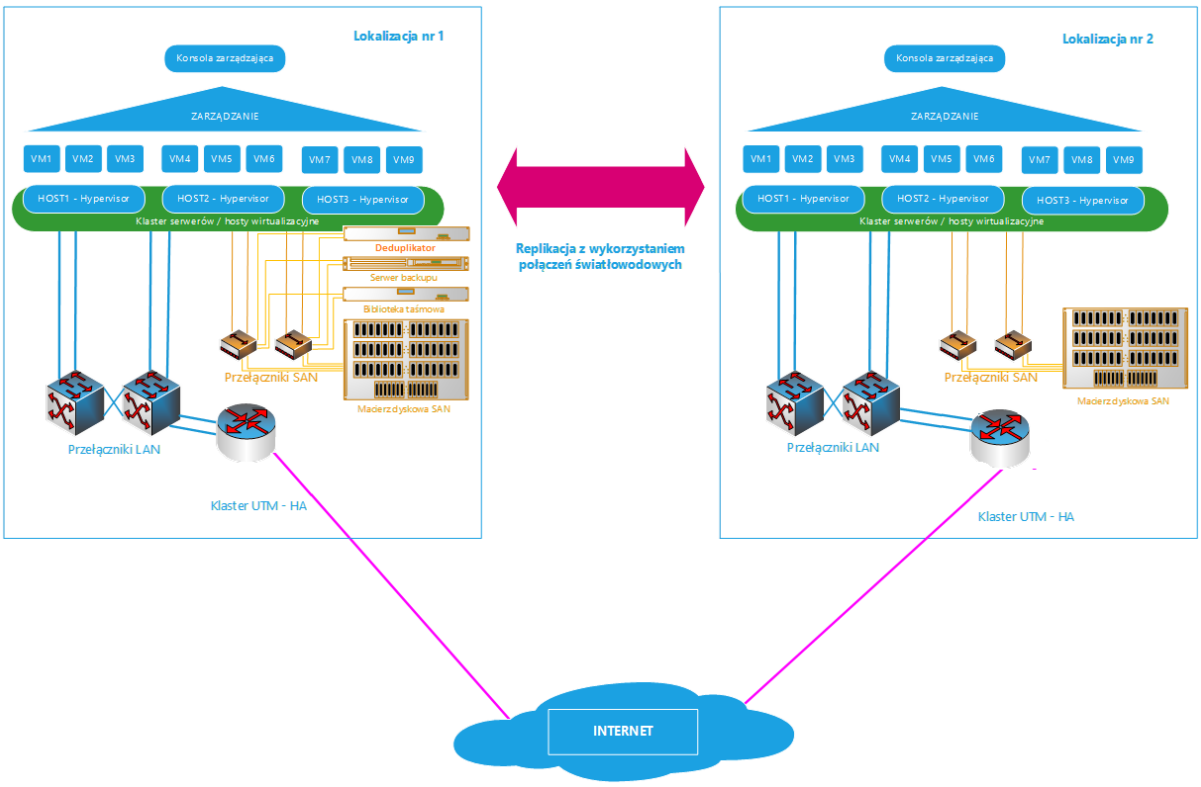
W ramach realizacji zostanie dostarczona i wdrożona infrastruktura informatyczna dla części regionalnej, niezbędna do jej uruchomienia i eksploatacji w okresie trwałości. Dotyczy to w szczególności serwerowni - Głównego Centrum Przetwarzania Danych GCPD (serwery z oprogramowaniem systemowym i narzędziowym, pamięci masowe, urządzenia archiwizujące, urządzenia transmisji danych, UTM/firewalle) umiejscowione w Lokalizacji nr 1 - siedzibie Urzędu Marszałkowskiego przy ul. Piłsudskiego 40.

Lokalizacja nr 2 GCPD umożliwi konfigurację klastra wysokodostępowego w trybie active-active. Aby zapewnić tryb HA, a jednocześnie zabezpieczyć środowisko przed zagrożeniami występującymi lokalnie, druga Lokalizacja GCPD powinna być połączona z pierwszą dedykowanym światłowodem. Serwerownia zapasowa zlokalizowana będzie w odległości ok. 100 m od GCPD zlokalizowanego w innej części Urzędu Marszałkowskiego przy ul. Piłsudskiego 40

Zadaniem części regionalnej jest zbieranie dokumentacji medycznej wytworzonej w systemach lokalnych. Repozytorium regionalne powinno spełniać wszystkie wymogi stawiane dla repozytoriów lokalnych, z którymi komunikacja powinna odbywać się automatycznie po wydzielonych, szyfrowanych łączach przy wykorzystaniu urządzeń umożliwiających zestawienie połączeń VPN lub innego bezpiecznego kanału komunikacji.

Głównym założeniem takiego repozytorium jest zarówno bezpieczne przechowywanie danych wytworzonych w jednostkach lokalnych, ale również udostępnianie dokumentacji.

Architektura rozwiązania:



Rys. Architektura rozwiązania

2. Serwery

Główne Centrum Przetwarzania Danych (GCPD) – budowa rozproszonego klastra niezwodnościowo-wydajnościowego, czyli instalacja środowiska wirtualnego na sześciu serwerach hostujących maszyny wirtualne, z czego trzy serwery będą znajdowały się w Lokalizacji nr 1, natomiast trzy pozostałe serwery w Lokalizacji nr 2. Dodatkowo elementem wchodzącym w skład klastra będzie zdublowana macierz dyskowa, replikująca dane synchronicznie oraz udostępniająca je w obu lokalizacjach jednocześnie (metrocluster).

Dostarczone serwery mają zostać połączone w klaster, który posłuży do obsługi wielu serwerów/maszyn wirtualnych VM zapewniając im odpowiedni poziom wydajności nawet w przypadku awarii, lub niedostępności, jednej z lokalizacji (Nr 1 lub Nr 2).

Ciągła dostępność dla serwera wirtualnego VM musi zostać zapewniona poprzez utworzenie i uruchomienie kopii maszyny wirtualnej VM (która jest identyczna i stale dostępna) w drugiej lokalizacji, tak aby móc zastąpić podstawową w przypadku awarii. Podstawowa maszyna wirtualna VM będzie w sposób ciągły replikowana do maszyny wirtualnej VM w drugiej lokalizacji, dzięki czemu kopia maszyny wirtualnej VM może przejąć ją w dowolnym momencie, zapewniając w ten sposób ochronę przed awariami.

W stworzonym środowisku zostanie uruchomiony Regionalny System Informatyczny jak również wszystkie usługi towarzyszące niezbędne do poprawnej pracy systemu.

3. Macierze

Dostarczone macierze dyskowe pod względem parametrów będą identyczne w obu lokalizacjach. W rozwiązaniu macierze będą udostępniały zasoby dyskowe dla potrzeb serwerów wirtualnych VM oraz przechowywały kopie zapasowe.

Należy uruchomić pomiędzy macierzami replikację synchroniczną, w celu zapewnienia odporności na awarię lub w przypadku niedostępności jednej z lokalizacji zapewnienia ciągłości działania.

Archiwizacja Regionalnego Repozytorium EDM (RREDM) będzie odbywać się z wykorzystaniem macierzy SAN oraz biblioteki taśmowej.

Do obsługi systemu kopii bezpieczeństwa dostarczony i wdrożony zostanie osobny serwer w Lokalizacji nr 1. Serwer ten wyposażony w przestrzeń dyskową, umożliwi tym samym przechowywanie najbardziej kluczowych systemów (maszyn wirtualnych) z zasobów dyskowych Flash macierzy. Pozwoli to, w razie konieczności, na ich szybkie odtworzenie. Backup danych przewidziany jest na macierzach oraz na bibliotece taśmowej (taśmy LTO9).

4. Przełączniki SAN zasobowe

Na potrzeby klastra wirtualizacyjnego należy zainstalować po dwa przełączniki SAN na każdą lokalizację, w celu połączenia urządzeń z zapewnieniem redundantności, aby awaria pojedynczego kontrolera w serwerze/macierzy nie powodowała jego wyłączenia z sieci.

5. Przełączniki LAN rdzeniowe

Przełączniki rdzeniowe mają za zadanie agregować ruch sieciowy: wszystkie połączenia z klastrów, pozostałych przełączników rdzeniowych, połączenia z dodatkowymi serwerowniami i kluczowymi punktami dystrybucyjnymi.

W obu lokalizacja Serwerowni przewidziane zostały dwa przełączniki rdzeniowe LAN połączone w stos z wykorzystaniem dedykowanych do tego celu modułów.

6. UTM

Zakłada się zastosowanie w każdej lokalizacji po jednym urządzeniu klasy UTM pracujących w klastrze. Rozwiązania Unified Threat Management pozwalają zabezpieczyć sieć na wielu płaszczyznach.

Dwa urządzenia będą pracowały wspólnie i będą zarządzane z poziomu jednego interfejsu. W przypadku awarii jednego z urządzeń pozostałe sprawne przejmie obsługę całej komunikacji w sposób niezauważalny tym samym utrzymując ciągłość działania.

II.1 Modernizacja sieci teleinformatycznej

1. Przedmiot zamówienia obejmuje zakup infrastruktury niezbędnej do modernizacji sieci teleinformatycznej oraz serwis gwarancyjny dostarczanych urządzeń przez okres zadeklarowany w ofercie.
2. Wykonawca zobowiązany jest dostarczyć i uruchomić kompleksową platformę dotycząca modernizacji sieci teleinformatycznej dla prawidłowego funkcjonowania Regionalnego Systemu Informatycznego
3. Dostawa i instalacja zostaną wykonane w lokalizacjach Zamawiającego zgodnie z Harmonogramem wdrożenia.
4. Modernizacja sieci teleinformatycznej musi zostać skonfigurowana tak, aby działała poprawnie zgodnie z jej przeznaczeniem i architekturą RSI oraz zapewniało prawidłową pracę Oprogramowania aplikacyjnego.
5. Infrastruktura musi być dostarczona do Zamawiającego, w terminie ustalonym z upoważnionym przedstawicielem Zamawiającego.

6. Wykonawca dostarczy i zainstaluje infrastrukturę zgodnie ze specyfikacją wymagań technicznych o parametrach minimalnych wymienionych poniżej.
7. Wszystkie urządzenia muszą być fabrycznie nowe - na dzień dostawy sprzęt nie może być starszy niż 9 miesięcy.
8. Zamawiający wymaga zainstalowania w/w systemów w miejscach wskazanych przez Zamawiającego.
9. Z uwagi na fakt, że realizacja zamówienia dotyczy obiektu użytkowanego, przed przystąpieniem do wykonywania jakichkolwiek robót, związanych z realizacją zamówienia, Wykonawca uzgodni z Zamawiającym terminy wykonywania robót. Ponadto, Wykonawca będzie zobowiązany do ścisłego współdziałania z upoważnionym przedstawicielem Zamawiającego podczas wykonywania robót w czynnym obiekcie lub w jego części, w celu zminimalizowania ograniczeń i uciążliwości związanych z wykonywanymi pracami, a w szczególności uzgadniania i ścisłego przestrzegania terminów oraz zakresów prowadzenia prac.
10. Zamawiający przed złożeniem oferty zaleca Wykonawcom dokonanie wizji lokalnej obiektu celem samodzielnej weryfikacji prac koniecznych do wykonania – dla prawidłowego oszacowania czasu realizacji wykonania przedmiotu zamówienia oraz jego wyceny. Zaleca się także dokonanie subiektywnego określenia na potrzeby wykonania wyceny i projektu oszacowania poziomu trudności prac i ilości koniecznych do zastosowania materiałów.
11. Wszelkie uszkodzenia infrastruktury ogólnej na obiekcie przez Wykonawcę podczas prowadzenia prac instalacyjnych obciążają jego samego i muszą być usunięte w ramach nieodpłatnego usunięcia szkód w terminie natychmiastowym po ich stwierdzeniu.
12. W okresie prowadzenia prac instalacyjnych i ich wykończenia Wykonawca zobligowany jest stosować się do przepisów i zasad zapewniających odpowiednie warunki wykonywania pracy i pobytu osób na terenie budowy, w tym także zapewniać poprawne oddziaływanie prowadzonych prac na środowisko, ze szczególnym uwzględnieniem przepisów BHP, ustawy o ochronie środowiska i ustawy o odpadach i stosownych przepisów wykonawczych. Zamawiający wymaga, aby Wykonawca we własnym zakresie zapewnił składowanie i sprzątanie odpadów.
13. W zakresie części modernizacji pomieszczenia serwerowni wymagane jest wykonanie następujących usług:
    1) **Szafa Rack - i**nstalacja fizyczna dostarczonych produktów:
        a) przygotowanie planu instalacji:
        b) zestawienie dostarczanych produktów,
        c) propozycję rozmieszczenia produktów w pomieszczeniu serwerowni,
        d) propozycję testów odbiorczych,
        e) montaż szafy rack w pomieszczeniu serwerowni.
    2) **Konsola KVM LCD**
        a) Instalacja i podłączenie konsoli KVM,
    3) **Urządzenie zabezpieczające UTM**
        a) Instalacja, montaż, uruchomienie oraz konfiguracja UTM-a:
            - montaż urządzenia w szafie rackowej,
            - podłączenie UTM-a do zasilania,
            - inicjalne uruchomienie UTM-a,
            - aktywacja licencji UTM-a,
            - testy działania UTM-a oraz weryfikacja parametrów,
            - podłączenie przełącznika do sieci LAN do przełączników LAN,
            - konfiguracja interfejsów sieciowych oraz interfejsu do zarządzania.
    4) **Przełączniki**
        a) Instalacja, montaż, uruchomienie oraz konfiguracja przełączników:
            - montaż przełączników w szafie rackowej,
            - podłączenie przełącznika do zasilania,
            - inicjalne uruchomienie przełącznika,

- testy działania przełącznika oraz weryfikacja parametrów,
- podłączenie przełącznika do sieci LAN i/lub SAN do istniejących przełączników LAN i/lub SAN,
- konfiguracja interfejsów sieciowych oraz interfejsu do zarządzania.

5) Wymagania ogólne

a) Wykonawca zainstaluje, podłączy, uruchomi i skonfiguruje w/w systemy,
b) Wykonawca po zrealizowaniu prac przeprowadzi min 2 godzinny instruktaż z zasad użytkowania i działania zamontowanych produktów.

Wymagane jest dostarczenie poniżej opisanych urządzeń o minimalnych parametrach funkcjonalnych:

II.1.1 UTM

Wymagane jest dostarczenie 2 szt. urządzeń UTM spełniających poniżej opisane minimalne parametry funkcjonalne:

Nazwa komponentu	Parametry techniczne
Wymagania Ogólne	1) Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. 2) System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym. 3) W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a,. Możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu. 4) System musi wspierać IPv4 oraz IPv6 w zakresie: a) Firewall, b) Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	1) W przypadku systemu pełniącego funkcje: Firewall – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2) Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3) Monitoring stanu realizowanych połączeń VPN. 4) System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP.
Interfejsy, Dysk, Zasilanie	1) System realizujący funkcję Firewall musi dysponować minimum: a) 8 portami Gigabit Ethernet RJ-45,

	b) 4 gniazdami SFP 1 Gbps, c) 2 gniazdami SFP+ 10 Gbps. 2) System Firewall musi posiadać wbudowany port konsoli szeregowej lub gniazdo USB. 3) W ramach systemu Firewall musi być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4) System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 480 GB. 5) System musi być wyposażony w zasilanie AC.
Parametry wydajnościowe	1) W zakresie Firewall'a obsługa nie mniej niż 1.5 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę. 2) Przepustowość Stateful Firewall: nie mniej niż 18 Gbps. 3) Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps. 4) Wydajność szyfrowania IPSec VPN nie mniej niż 9 Gbps. 5) Wydajność skanowania ruchu w celu ochrony przed (w ramach modułu IPS) - minimum 2.5 Gbps. 6) Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.
Funkcje Systemu Bezpieczeństwa	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1) Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2) Kontrola Aplikacji. 3) Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4) Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5) Ochrona przed atakami - Intrusion Prevention System. 6) Kontrola stron WWW. 7) Zarządzanie pasmem (QoS, Traffic shaping). 8) Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 9) Analiza ruchu szyfrowanego protokołem SSL.
Polityki, Firewall	1) Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2) System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: a) translację jeden do jeden oraz jeden do wielu, 3) W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
Połączenia VPN	1) System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: a) wsparcie dla IKE v1 oraz v2,

	b) obsługa szyfrowania protokołem AES z kluczem 128 i 256, c) wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, d) tworzenie połączeń typu Site-to-Site oraz Client-to-Site, e) monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności, f) możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego, g) obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth, 2) System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: h) pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki, i) pracę w trybie Tunnel, j) producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie powinno zapewniać obsługę: a) Routingu statycznego, b) Policy Based Routingu, c) Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP.
Zarządzanie pasmem	1) System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma. 2) Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3) System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	1) Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji. 2) System musi umożliwiać skanowanie archiwów. 3) System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 4) System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
Ochrona przed atakami	1) Ochrona IPS musi opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2) System musi chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3) Baza sygnatur ataków musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4) Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5) System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami

	typu DoS oraz DDoS. 6) Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: SQL Injecton. 7) Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
Kontrola aplikacji	1) Baza Kontroli Aplikacji musi zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 2) Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) muszą być kontrolowane pod względem wykonywanych czynności. 3) Baza musi zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: P2P. 4) Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
Kontrola WWW	1) Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 20 milionów adresów URL pogrupowanych w kategorie tematyczne. 2) W ramach filtra www muszą być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania). 3) Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4) Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5) W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	1) System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: a) haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu, b) haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP, c) haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2) Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
Zarządzanie	1) Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2) Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3) Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4) System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk

	ruchu za pomocą protokołów netflow lub sflow. 5) System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API. 6) Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
Logowanie	1) Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2) W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3) Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4) Musi istnieć możliwość logowania do serwera SYSLOG.
Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa muszą posiadać następujące certyfikacje: ICSA lub EAL4 dla funkcji Firewall lub równoważne (rekomendacja respektowana przez NATO i Unię Europejską NATO Restricted i UE Restricted).
Serwisy i licencje	W ramach postępowania muszą zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Będą one obejmować: Kontrolę Aplikacji, IPS, Analizę typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy.
Gwarancja oraz wsparcie	Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne producenta w trybie 24x7.
Opisy do wymagań ogólnych	1) Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu

	do produktów podwójnego zastosowania. 2) Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

II.1.2 Przełącznik serwerowy LAN

Wymagane jest dostarczenie 4 szt. przełączników LAN spełniających poniżej opisane minimalne parametry funkcjonalne:

Nazwa komponentu	Opis wymagań
Typ	Przełącznik sieciowy zarządzalny rack SFP+.
Porty	1) Minimum 24 porty 1G/10G SFP+. 2) Minimum 2 porty QSFP28 z możliwością pracy 40Gbit/100Gbit. 3) Port konsoli. 4) Minimum 1 port USB. 5) Porty SFP+ muszą umożliwiać ich obsadzanie wkładkami 10 Gigabit Ethernet. 6) Możliwość łączenia w stos przełączników.
Parametry fizyczne	Wysokość maksymalnie 1U, montowany w szafie typu rack 19'', redundantny zasilacz.
Pamięć	1) Co najmniej 4GB pamięci DDR. 2) Co najmniej 8GB pamięci flash.
Wielkość tablicy adresów MAC	Co najmniej 32 000.
Ilość obsługiwanych sieci VLAN	Co najmniej 4094.
Wydajność	1) Przepustowość przełączania: min. 880 Gbit/s. 2) Przełączanie dla pakietów: min. 654Mpps.
Obsługa ramek Jumbo	O wielkości co najmniej 9198 bajtów.

Funkcjonalność urządzenia	1) Obsługa agregacji portów zgodnie z LACP (IEEE 802.3ad). 2) Wbudowany DHCP Serwer i klient 3) Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash 4) Możliwość monitorowania zajętości CPU 5) 6) Obsługa protokołu NTP. 7) Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree. 8) Musi być wyposażone w port USB umożliwiający podłączenie pamięci flash. 9) Musi mieć możliwość zarządzania poprzez interfejs CLI z poziomu portu konsoli. 10) Musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN. 11) Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją.
Bezpieczeństwo	1) Możliwość integracji funkcjonalności Network Login z systemem NAC (Network Access Control) 2) Przydział sieci VLAN, ACL/QoS podczas logowania Network Login 3) Obsługa RADIUS (RFC 2139) 4) Ograniczenie liczby MAC adresów na porcie 5) Możliwość wpisania statycznych MAC adresów na port/vlan 6) Obsługa SNMPv1/v2/v3 7) Klient SSH2 8) Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika 9) Obsługa DHCP 10) Obsługa Trusted DHCP Server 11) Obsługa DHCP Snooping 12)
Wsparcie dla mechanizmów zapewnienia jakość usług w sieci	1) Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie co najmniej następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP. 2) Implementacja co najmniej czterech kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. 3) Możliwość obsługi jednej z powyżej wymienionych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority). 4) Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi.

Zasilanie	1) Zasilacz wymieniany hot-swap. 2) Możliwość zastosowania redundantnego zasilacza wewnętrznego 3) Switch należy dostarczyć razem z dodatkowym zasilaczem redundantnym. 4) Przełącznik dodatkowo musi posiadać wentylację.
Akcesoria	Razem z przełącznikami należy dostarczyć: 1) Kabel Stack do portu 100 Gb, QSFP28 o długości 3m do zestawienia stack lub dedykowany kabel do zestawienia stack, 2) Niezbędne wkładki 10Gbit SFP+ oraz kable w celu podłączenia dostarczonego sprzętu.
Gwarancja	1) 60 miesięczna gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory). 2) Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.
Zarządzanie	1) Urządzenia muszą być w pełni kontrolowane i zarządzane za pomocą istniejącego systemu Extreme Networks NetSight. Zamawiający dopuszcza dostarczenie i uruchomienie równoważnego systemu. Poprzez równoważność należy rozumieć funkcjonalności nie mniejsze niż Extreme Networks NetSight w zakresie: • Szczegółowe informacje o tożsamości i dostępie, • Raporty, • mapy topologii sieci, • Widoki urządzeń oraz zarządzanie alarmami i zdarzeniami dla całej infrastruktury. • Diagnostyka umożliwiając diagnozowanie problemów sieciowych i wydajności poprzez analizę w czasie rzeczywistym. • Zarządzanie polityką • Zarządzanie kontrolą dostępu do sieci • Zarządzanie zapasami • Zautomatyzowane zarządzanie bezpieczeństwem • Zautomatyzowane tworzenie kopii konfiguracji urządzeń W przypadku dostarczenia systemu równoważnego Zamawiający wymaga dostarczenia dodatkowych 50 licencji do zarządzania posiadanymi przez Zamawiającego switchami Extreme Networks X590-24x-1q2c (Enterasys).
Dokumenty	Wykonawca winien przedłożyć dokumenty: 1) Oferowane urządzenie musi posiadać certyfikat CE oraz deklarację zgodności CE lub musi być oznaczony znakiem CE (oświadczenie Wykonawcy w Formularzu ofertowym), 2) Oświadczenie producenta lub oświadczenie autoryzowanego przedstawiciela producenta potwierdzające zgodność wszystkich parametrów oferowanego urządzenia wskazanych w Opisie przedmiotu zamówienia.

Instruktaże	Wymagane jest przeprowdzenie dedykowanych instruktaży dla 6 pracowników Zamawiającego po uruchomieniu urządzeń. Instruktaż ma na celu przekazanie wiedzy wymaganej do administrowania i zarządzania oferowanymi przełącznikami LAN. Instruktaż musi być przeprowadzony przez wykwalifikowanych inżynierów posiadających certyfikaty inżyniera producenta oferowanych przełączników LAN. Instruktaż może być przeprowadzony na miejscu u Zamawiającego, bądź online. Instruktaż w wymiarze minimum 21 godzin zegarowych musi zawierać przynajmniej 40% czasu w formie warsztatów praktycznych/laboratoriów dla uczestników. Terminy instruktaży zostaną ustalone z Zamawiającym.

II.1.3 Przełącznik zasobowy SAN

Wymagane jest dostarczenie 4 szt. przełączników SAN spełniających opisane poniżej minimalne parametry funkcjonalne:

Lp.	Opis wymagań
1.	Przełącznik FC musi być wykonany w technologii FC minimum 32 Gb/s i zapewniać możliwość pracy portów FC z prędkościami 32, 16, 8, 4 Gb/s w zależności od rodzaju zastosowanych wkładek SFP.
2.	W przypadku obsadzenia portu FC za pomocą wkładki SFP 32Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 32, 16 lub 8 Gb/s, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji.
3.	W przypadku obsadzenia portu FC za pomocą wkładki SFP 16Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 16, 8 lub 4 Gb/s, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji.
4.	Przełącznik FC musi być wyposażony, w co najmniej 24 aktywnych portów FC obsadzonych minimum wkładkami SFP 32Gb/s.
5.	Wszystkie zaoferowane porty przełącznika FC muszą umożliwiać działanie bez tzw. oversubscrypcji gdzie wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika mogą pracować równocześnie z pełną prędkością 16Gb/s lub 32Gb/s w zależności od zastosowanych wkładek FC.
6.	Całkowita przepustowość przełącznika FC dostępna dla maksymalnie rozbudowanej konfiguracji (24 porty) wyposażonej we wkładki 32Gb/s musi wynosić minimum 768 Gb/s end-to-end.
7.	Oczekiwana wartość opóźnienia przy przesyłaniu ramek FC między dowolnymi portami przełącznika nie może być większa niż 900ns.
8.	Rodzaj obsługiwanych portów, co najmniej: E, D oraz F.
9.	Przełącznik FC musi mieć wysokość maksymalnie 1 U (jednostka wysokości szafy montażowej) i szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”.
10.	Przełącznik FC musi być wyposażony w mechanizm agregacji połączeń ISL między dwoma przełącznikami i tworzenia w ten sposób logicznych połączeń typu ISL Trunk o przepustowości minimum 256 Gb/s half duplex (dla wkładek 32Gbps) dla każdego logicznego połączenia. Load balancing ruchu między fizycznymi połączeniami ISL w ramach połączenia logicznego typu trunk musi być realizowany na poziomie pojedynczych ramek FC a połączenie logiczne musi zachowywać kolejność przesyłanych ramek. Należy dostarczyć odpowiednią licencję jeżeli jest wymagana.
11.	Przełącznik FC musi wspierać mechanizm balansowania ruchu, pomiędzy co najmniej 16

	różnymi ścieżkami o tym samym koszcie wewnątrz wielodomenowych sieci fabric, przy czym balansowanie ruchu musi odbywać się w oparciu o 3 parametry nagłówka ramki FC: DID, SID i OXID.
12.	Przełącznik FC musi zapewniać jednoczesną obsługę mechanizmów ISL Trunk oraz balansowania ruchu w oparciu o DID/SID/OXID. Należy dostarczyć odpowiednią licencję, jeżeli jest wymagana.
13.	Przełącznik FC musi realizować sprzętową obsługę zoningu (przez tzw. układ ASIC) na podstawie portów i adresów WWN.
14.	Przełącznik FC musi wspierać następujące mechanizmy zwiększające poziom bezpieczeństwa: 1) mechanizm tzw. Fabric Binding, który umożliwia zdefiniowanie listy kontroli dostępu regulującej prawa przełączników FC do uczestnictwa w sieci fabric, 2) uwierzytelnianie (autentykacja) przełączników w sieci Fabric za pomocą protokołów DH-CHAP i FCAP, 3) uwierzytelnianie (autentykacja) urządzeń końcowych w sieci Fabric za pomocą protokołu DH-CHAP, 4) szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2, 5) definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control), 6) definiowane kont administratorów w środowisku RADIUS, LDAP w MS Active Directory, Open LDAP, TACACS+, 7) szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS, 8) obsługa SNMP v1 oraz v3, 9) IP Filter dla portu administracyjnego przełącznika, 10) wgrywanie nowych wersji firmware przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP, 11) wykonywanie kopii bezpieczeństwa konfiguracji przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP.
15.	Przełącznik FC musi mieć możliwość konfiguracji przez: 1) polecenia tekstowe w interfejsie znakowym konsoli terminala, 2) przeglądarkę internetową z interfejsem graficznym lub dedykowane oprogramowanie.
16.	Przełącznik FC musi być wyposażony w następujące narzędzia diagnostyczne i mechanizmy obsługi ruchu FC: 1) logowanie zdarzeń poprzez mechanizm „syslog”, 2) ciągłe monitorowanie parametrów pracy przełącznika, portów, wkładek SFP i sieci fabric z automatycznym powiadamianiem administratora, wyłączeniem pracy portu lub przesunięciem przepływów tzw. slow drain na niski priorytet w przypadku przekroczenia zdefiniowanych wartości granicznych. Powiadamianie administrator musi być możliwe za pomocą wysyłania wiadomości e-mail, pułapki SNMP lub komunikatu w logu. Należy dostarczyć odpowiednią licencję jeżeli jest wymagana, 3) port diagnostyczny tzw. D_port. Port diagnostyczny musi umożliwiać wykonanie testów sprawdzających komunikację portu przełącznika z wkładką SFP, połączenie optyczne pomiędzy dwoma przełącznikami, testowe obciążenie połączenia pełną przepustowością 16Gbps/32Gbps oraz pomiar opóźnienia i odległości między przełącznikami z dokładnością co najmniej do 5m dla wkładek SFP 16Gbps lub 32Gbps. Testy wykonywane przez port diagnostyczny nie mogą wpływać w żaden sposób na

	działanie pozostałych portów przełącznika i całej sieci fabric, 4) FCping, 5) FC traceroute, 6) kopiowanie danych wymienianych pomiędzy dwoma wybranymi portami na inny wybrany port przełącznika, 7) Przełącznik musi być wyposażony w mechanizm sprzętowego monitorowania przepływów danych dla wskazanych jak i automatycznie wykrywanych par urządzeń komunikujących się przez dany port przełącznika. Dla każdego monitorowanego przepływu muszą być gromadzone statystyki dotyczące, co najmniej liczby wysłanych i odebranych ramek, przepustowości, liczby zapisów i odczytów SCSI, przy czym musi istnieć możliwość zawężenia zakresu monitorowania do następujących typów ramek: SCSI Reserve, SCSI Aborts, SCSI Read, SCSI Write, rejected frames. Należy dostarczyć odpowiednią licencję jeżeli jest wymagana, 8) Przełącznik musi być wyposażony w mechanizm sprzętowego generatora ruchu umożliwiającego symulowanie komunikacji w wielodomenowych sieciach SAN bez konieczności angażowania fizycznych urządzeń takich jak serwery lub macierze dyskowe. Należy dostarczyć odpowiednią licencję jeżeli jest wymagana, 9) Przełącznik musi być wyposażony w mechanizm umożliwiający kopiowanie pierwszych 64 bajtów ramek dla wybranych przepływów danych do pamięci lokalnej przełącznika w celu dalszej analizy, 10) Przełącznik musi być wyposażony w mechanizm umożliwiający sprzętowe identyfikowanie ramek FC oznaczonych parametrem VM ID oraz integrację tego mechanizmu z systemami monitorowania przepływów danych w szczególności w zakresie przepustowości oraz liczby zapisów i odczytów na sekundę,
17.	Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet.
18.	Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S.
19.	Przełącznik FC musi realizować kategoryzację ruchu między parami urządzeń (initiator - target) oraz przydzielenie takich par urządzeń do kategorii o wysokim, średnim lub niskim priorytecie. Konfiguracja przydziału do różnych klas priorytetów musi się odbywać za pomocą standardowych narzędzi do konfiguracji zoningu.
20.	Przełącznik FC musi realizować kategoryzację ruchu na podstawie wartości parametru CS_CTL w nagłówku ramki FC oraz odpowiednie przydzielenie ramki do kategorii o wysokim, średnim lub niskim priorytecie.
21.	Wsparcie dla N_Port ID Virtualization (NPIV). Obsługa, co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika.
22.	Support/Gwarancja: Wymagana jest gwarancja świadczona w trybie 24 godziny przez 7 dni w tygodniu na wszystkie elementy (sprzęt oraz oprogramowanie) na okres 60 miesięcy. Zamawiający wymaga, aby usługi serwisowe świadczone były wyłącznie przez producenta oferowanego sprzętu, nie dopuszcza się świadczenia serwisu przez autoryzowanych partnerów producenta (wymagane oświadczenie producenta).

II.1.4 Szafa 42U z wyposażeniem

Wymagane jest dostarczenie 2 szt. szafy rack spełniającej poniżej opisane minimalne parametry funkcjonalne:

Nazwa elementu, parametru lub cechy	Opis wymagań
Rodzaj	W pełni montowana szafa serwerowa stojąca typu Rack.
Wysokość	42U
Szerokość całkowita	Min. 800 mm
Głębokość całkowita	Min. 1060 mm
Szerokość szyn montażowych	482,6 mm (19 cali).
Ilość belek nośnych	Dwie pary belek nośnych 19 cali z możliwością regulacji położenia.
Wykonanie drzwi przednich	Blaszane, jednoskrzydłowe, perforowane z zamkiem z klamką.
Wykonanie drzwi tylnych	Blaszane, dwuskrzydłowe, perforowane z zamkiem z klamką.
Ściągane panele boczne	Tak, dwie osłony boczne, pełne, z zamkami.
Kółka transportowe	Tak
Stopki poziomujące	Tak
Numeracja jednostek U na belkach nośnych	Tak, na belkach przednich i tylnych.
Dedykowany kanał na listwę PDU	Tak, dedykowany pionowy kanał lub uchwyt umożliwiający zamontowanie pionowych listew PDU.
Listwa zasilająca PDU	Liczba, typ gniazd wyjściowych: 4 szt. IEC-320-C19 + 20 szt. IEC-320-C13 Prąd znamionowy listy: 32A Zdalne zarządzanie poprzez sieć Ethernet – przełączanie gniazd wyjściowych, pomiary parametrów elektrycznych listwy.
Obciążenie statyczne (na stopkach poziomujących)	1000kg
Gwarancja producenta	60 miesiące

II.1.5 Konsola KVM-KMM

Wymagane jest dostarczenie 2 szt. konsoli KVM-KMM spełniającej poniżej opisane minimalne parametry funkcjonalne:

Nazwa elementu, parametru lub cechy	Opis wymagań
Ogólne właściwości użytkowe	1) Składana, wysuwana konsola przystosowana do montażu w szafie Rack. 2) Urządzenie musi posiadać wbudowany ekran LCD o przekątnej minimum 18”. 3) Urządzenie musi posiadać wbudowaną klawiaturę z układem US (qwerty). 4) Urządzenie musi posiadać wbudowaną mysz minimum dwuprzyciskową w formie trackball lub touchpad. 5) Urządzenie musi posiadać wbudowany przełącznik KVM umożliwiający podpięcie minimum 8 urządzeń zewnętrznych bezpośrednio za pośrednictwem okablowanie VGA i portów USB 6) Zmiana sygnału wejściowego oraz przekierowanie urządzeń wyjściowych musi być realizowane z poziomu przycisków umieszczonych w łatwo dostępnym miejscu urządzenia. 7) Konsola musi być wyposażona w szyny montażowe pozwalające na instalację w szafie Rack. Szyny muszą umożliwiać korzystanie z konsoli KVM przy zajętości sąsiednich miejsc instalacyjnych w szafie – pełne wysunięcie oraz otwarcie urządzenia. 8) Monitor LCD musi uruchamiać się w chwili podniesienia konsoli do pracy operacyjnej. 9) Należy zapewnić niezbędne kable przyłączeniowe do przełącznika KVM w ilości 8 szt.
Gwarancja	60 miesięcy

II.2 Dostawa i wdrożenie Infrastruktury Serwerowej

1. Wykonawca zobowiązany jest dostarczyć i uruchomić kompleksową platformę Infrastruktury serwerowej (serwery, macierze wraz z niezbędnym Oprogramowaniem Narzędziowym – systemowym, bazodanowym, wirtualizacyjnym, backupowym i pozostałym oprogramowaniem) dla prawidłowego funkcjonowania Regionalnego Systemu Informatycznego.
2. Dostawa i instalacja zostaną wykonane w lokalizacjach Zamawiającego zgodnie z Harmonogramem wdrożenia.
3. Infrastruktura serwerowa musi zostać skonfigurowane tak, aby działała poprawnie zgodnie z jej przeznaczeniem i architekturą RSI oraz zapewniało prawidłową pracę Oprogramowania aplikacyjnego.
4. Infrastruktura musi być dostarczona do Zamawiającego, w terminie ustalonym z upoważnionym przedstawicielem Zamawiającego.
5. Jeżeli zajdzie potrzeba, wraz z dostarczoną Infrastrukturą Serwerową, Wykonawca zobowiązany jest dostarczyć niezbędne elementy np. urządzenia i wyposażenie – kable połączeniowe, elementy mocujące, uznane przez Wykonawcę za niezbędne i umożliwiające prawidłowe działanie całego Systemu. Dostarczona Infrastruktura Serwerowa musi zapewniać bezproblemową pracę po podłączeniu jej do sieci informatycznej Zamawiającego.

6. Wykonawca jest zobowiązany dokonać montażu dostarczonej Infrastruktury Serwerowej oraz oprogramowania w miejscach wskazanych przez Zamawiającego.
7. Wszystkie elementy Infrastruktury serwerowej muszą zostać zamontowane w szafie serwerowej rack, w sposób umożliwiający ich prawidłową wentylację.
8. Szczegóły dotyczące instalacji i uruchomienia Infrastruktury serwerowej zostaną ustalone w trakcie Analizy Przedwdrożeniowej.
9. Zamawiający umożliwia odbycie wizji lokalnej Wykonawcy Wizja lokalna może odbyć się w pracujące dni powszednie (poniedziałek – piątek) w zakresie godzin od …. do ….. po uzgodnieniu konkretnego terminu z Zamawiającym.
10. Wykonawcy, którzy są zainteresowani przeprowadzeniem ww. wizji lokalnej w celu zapoznania się z obiektem, zobowiązani są zgłosić chęć uczestniczenia w wizji lokalnej za pośrednictwem mail na adres: …….. O terminie przeprowadzenia wizji lokalnej Wykonawcy zostanie poinformowany mailem.
11. W zakresie części serwerowej w ramach postępowania wymagane jest wykonanie następujących usług:
    1) Instalacja fizyczna dostarczonej Infrastruktury:
        a) Przygotowanie planu instalacji:
            - zestawienie dostarczanych urządzeń,
            - propozycję rozmieszczenia elementów w istniejących szafach rackowych,
            - propozycję testów odbiorczych,
        b) Instalacja, montaż i uruchomienie serwerów wirtualizacyjnych:
            - montaż serwera w istniejącej szafie rackowej,
            - podłączenie serwera do przełącznika KVM,
            - podłączenie serwera do sieci LAN i/lub SAN do przełączników LAN i/lub SAN,
            - podłączenie serwera do zasilania,
            - inicjalne uruchomienie serwera,
            - testy działania serwera oraz weryfikacja parametrów,
        c) Instalacja, montaż i uruchomienie macierzy dyskowej:
            - montaż macierzy w szafie rackowej,
            - podłączenie macierzy do sieci LAN i/lub SAN,
            - inicjalne uruchomienie macierzy,
            - testy działania macierzy oraz weryfikacja parametrów.
        d) Instalacja, montaż i uruchomienie biblioteki taśmowej:
            - montaż biblioteki taśmowej w szafie rackowej,
            - podłączenie biblioteki taśmowej do sieci LAN i/lub SAN,
            - inicjalne uruchomienie biblioteki taśmowej,
            - testy działania biblioteki taśmowej oraz weryfikacja parametrów.
        e) Instalacja, montaż i uruchomienie systemu backupu:
            - montaż serwera/deduplikatora/biblioteki taśmowej w szafie rackowej,
            - podłączenie serwera backupu do przełącznika KVM,
            - podłączenie urządzenia do sieci LAN i/lub SAN do przełączników LAN i/lub SAN,
            - podłączenie systemu backupu do zasilania,

- inicjalne uruchomienie systemu backupu,
- testy działania oraz weryfikacja parametrów,

2) Konfiguracja macierzy dyskowej:
   a) Przygotowanie planu rozbudowy:
      - zestawienie stosowanej nomenklatury,
      - zestawienie serwerów, które będą korzystać z wystawianych zasobów,
      - weryfikacja poziomów mikrokodów,
      - zestawienie wymaganych wersji oprogramowania/łat systemowych po stronie serwerów,
      - przygotowanie szczegółowej koncepcji konfiguracji dysków macierzy odzwierciedlającej potrzeby biznesowe,
      - zestawienie zakupionego oprogramowania,
      - propozycja testów odbiorczych,
   b) Implementacja zgodna z projektem:
      - instalacja sprzętowa,
      - aktywacja zakupionego oprogramowania,
      - konfiguracja replikacji synchronicznej – jeżeli dotyczy,
      - implementacja zaakceptowanej konfiguracji logicznej macierzy,
   c) Testy odbiorcze:
      - zestawienie stosowanej nomenklatury,
      - weryfikację zgodności z planem wdrożenia,
      - przeprowadzenie testów potwierdzających poprawność instalacji macierzy,
   d) Przygotowanie dokumentacji powykonawczej:
      - zestawienie stosowanej nomenklatury,
      - zestawienie serwerów korzystających z wystawianych zasobów,
      - zestawienie poziomów mikrokodów,
      - zestawienie wymaganych wersji oprogramowania/łat systemowych po stronie serwerów,
      - zestawienie konfiguracji dysków macierzy,
      - zestawienie mapowania udostępnionych zasobów,
      - zestawienie zakupionego i aktywowanego oprogramowania,
      - definicje testów odbiorczych.
3) Instalacja oprogramowania wirtualizacyjnego, systemowego oraz backupowego:
   a) Inwentaryzacja stanu obecnego:
      - zestawienie nazewnictwa poszczególnych elementów istniejącego systemu,
      - zestawienie zainstalowanych łat systemu operacyjnego,
      - zestawienie zainstalowanych wersji oprogramowania,
   b) Przygotowanie projektu technicznego:
      - zestawienie stosowanej nomenklatury,
      - rysunki logicznej struktury systemu,
      - propozycję nazewnictwa poszczególnych elementów systemu wirtualizacji,
      - zestawienie wymaganych wersji oprogramowania,
      - propozycje konfiguracji systemu wirtualizacji,

- propozycje konfiguracji systemów operacyjnych,
- propozycje konfiguracji systemu backupowego – jeżeli dotyczy.

c) Implementacja zgodna z projektem:
- instalacja oprogramowania wirtualizacyjnego, systemowego oraz backupowego,
- konfiguracja oprogramowania wirtualizacyjnego, systemowego oraz backupowego,
- aktywacja dostarczonego oprogramowania,

d) Przygotowanie dokumentacji powykonawczej zawierającej:
- zestawienie stosowanej nomenklatury,
- rysunki logicznej struktury systemu wirtualizacji i backupu,
- zestawienie nazewnictwa poszczególnych elementów systemu,
- zestawienie konfiguracji systemu wirtualizacji,
- zestawienie wersji zainstalowanego oprogramowania systemowego oraz backupowego.

12. Po zakończonym montażu Wykonawca przekaże Zamawiającemu wszystkie hasła dostępowe do kont „super użytkowników" oraz dokumentację do wszystkich oferowanych urządzeń, oprogramowania narzędziowego (systemowego, bazodanowego, wirtualizacyjnego, backupowego itd.) wraz z dokumentami potwierdzającymi nabycie dla Zamawiającego licencji oraz nośnikami danych zawierającymi zainstalowane oprogramowanie. Wykonawca wykona również instruktaże użytkowe dla wskazanego przez Zamawiającego administratora, z zakresu konfiguracji, obsługi i prawidłowej eksploatacji zainstalowanego Sprzętu ze szczególnym uwzględnieniem obsługi i zaawansowanego zarządzania macierzą danych, w środowisku Zamawiającego.
13. Wykonawca zobowiązany jest zapewnić 60 miesięczne wsparcie i możliwość prowadzenia konsultacji w zakresie administracji zaoferowanym sprzętem oraz dostarczonym oprogramowaniem narzędziowym (systemowym, wirtualizacyjnym i bazodanowym) z osobami wskazanymi przez Wykonawcę, posiadającymi odpowiednie certyfikaty producentów urządzeń i oprogramowania na warunkach gwarancji producenta lub dostawcy sprzętu. Pozostałe wymagania dotyczące gwarancji zostały opisane w OPZ w rozdziale III. Gwarancja.
14. Wszystkie urządzenia muszą być fabrycznie nowe - na dzień dostawy sprzęt nie może być starszy niż 9 miesięcy.

II.2.1 Serwer lokalizacja nr 1

Wymagane jest dostarczenie 3 szt. serwerów spełniających poniżej opisane minimalne parametry funkcjonalne:

Nazwa komponentu	Opis wymagań
Obudowa	1) Obudowa typu RACK o wysokości maksymalnie 2U, przystosowana do montażu w szafie stelażowej 19". 2) Wraz z obudową wymagany jest komplet szyn umożliwiających montaż w szafie RACK 19" oraz wysuwanie serwera do celów serwisowych.
Płyta główna	Płyta główna zaprojektowana do pracy w serwerach, z możliwością

	zainstalowania minimum dwóch procesorów oraz możliwością obsługi min. 2 TB pamięci RAM.
Procesor	Zainstalowane 2 procesory min. 16-rdzeniowe, w architekturze x86 osiągające wynik min. 220 pkt w testach wydajności SPECrate2017_int_base (www.spec.org) w dniu publikacji.
Pamięć RAM	1) Minimum 512 GB pamięci RAM typu RDIMM 2933MT/s 2) Wsparcie dla technologii zabezpieczania pamięci, min: ECC
Pamięć masowa	Zatoki dyskowe gotowe do zainstalowania 8 dysków SFF typu Hot Swap, SAS/SATA/SSD, 2,5". Zainstalowane dwa dyski SSD minimum 240 GB.
Kontroler dyskowy	Kontroler SAS sprzętowy wspierany przez oprogramowanie do wirtualizacji. Możliwość instalacji kontrolera sprzętowego z min. 2GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniającego obsługę 8 napędów dyskowych SAS oraz obsługujący poziomy: RAID 0/1/10/5/50/6/60.
Interfejsy	Minimum 4 porty USB; minimum 1 x port graficzny z tyłu obudowy.
Interfejsy sieciowe	1) Minimum 4 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ z modułami SFP+ SR. 2) Minimum 2 interfejsy zapewniające prędkość połączenia minimum 32Gb/s typu FC16 oraz sześć kabli światłowodowych LC-LC o długości min. 3m.
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200, dedykowana pamięć układu graficznego min. 16MB.
Porty rozszerzeń	2 gniazda PCI-Express generacji 3 lub 4 dla kart rozszerzeń.
Wentylatory	Redundantne wentylatory typu Hot-Plug.
Zasilanie	Redundantne zasilacze Hot Plug o mocy min. 800W każdy.
Bezpieczeństwo	Zintegrowany panel diagnostyczny LCD lub zestaw diod LED umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o statusie serwera. Serwer wyposażony w moduł TPM 2.0.
Zarządzanie	Serwer musi posiadać moduł zarządzający wyposażony w minimum jeden port 10/100/1000 Base-T Ethernet, pozwalający na zdalny dostęp i zarządzanie serwerem przy użyciu graficznego interfejsu Web. Moduł musi umożliwiać: 1) monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe, 2) dostęp do karty zarządzającej poprzez: a) dedykowany port RJ45 z tyłu serwera, 3) dostęp do karty możliwy: a) z poziomu linii komend, b) poprzez interfejs IPMI 2.0, 4) wbudowane narzędzia diagnostyczne, 5) zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego, 6) obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie, 7) wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej

	w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników, 8) przesyłanie alertów poprzez e-mail, 9) obsługa zdalnego serwera logowania (remote syslog), 10) wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów CD/DVD 11) monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji, 12) konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping), 13) zdalna aktualizacja oprogramowania (firmware), 14) możliwość równoczesnej obsługi przez min. 2 administratorów, 15) wsparcie dla Microsoft Active Directory, 16) obsługa TLS i SSH, 17) wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 18) Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną, posiadające dedykowany port RJ45. Całe rozwiązanie z oprogramowaniem do zdalnego zarządzania serwerem musi być produktem pochodzącym od producenta serwera oraz musi być objęte wsparciem producenta serwera.
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	1) Microsoft Windows Server 2016, 2019. 2) Red Hat Enterprise Linux (RHEL) 8. 3) SUSE Linux Enterprise Server (SLES) 15. 4) VMware ESXi 6.x, 7.x.
Certyfikaty	1) Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. 2) Oferowane urządzenie musi posiadać certyfikat CE oraz deklarację zgodności CE lub musi być oznaczony znakiem CE (oświadczenie Wykonawcy w Formularzu ofertowym).
Gwarancja	1) 60 miesięcy. 2) Usługa wsparcia technicznego musi być świadczona przez autoryzowany serwis producenta oferowanych urządzeń. 3) Uszkodzone dyski twarde pozostają własnością Zamawiającego.

II.2.2 Serwer lokalizacja nr 2

Wymagane jest dostarczenie 3 szt. serwerów spełniających poniżej opisane minimalne parametry funkcjonalne:

Nazwa komponentu	Opis wymagań
Obudowa	1) Obudowa typu RACK o wysokości maksymalnie 2U, przystosowana do montażu w szafie stelażowej 19”. 2) Wraz z obudową wymagany jest komplet szyn umożliwiających montaż w szafie RACK 19” oraz wysuwanie serwera do celów serwisowych.

Płyta główna	Płyta główna zaprojektowana do pracy w serwerach, z możliwością zainstalowania minimum dwóch procesorów oraz możliwością obsługi min. 2 TB pamięci RAM.
Procesor	Zainstalowane 2 procesory min. 16-rdzeniowe, w architekturze x86 osiągające wynik min. 220 pkt w testach wydajności SPECrate2017_int_base (www.spec.org) w dniu publikacji.
Pamięć RAM	1) Minimum 512 GB pamięci RAM typu RDIMM 2933MT/s 2) Wsparcie dla technologii zabezpieczania pamięci, min: ECC
Pamięć masowa	Zatoki dyskowe gotowe do zainstalowania 8 dysków SFF typu Hot Swap, SAS/SATA/SSD, 2,5". Zainstalowane dwa dyski SSD minimum 240 GB.
Kontroler dyskowy	Kontroler SAS sprzętowy wspierany przez oprogramowanie do wirtualizacji. Możliwość instalacji kontrolera sprzętowego z min. 2GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniającego obsługę 8 napędów dyskowych SAS oraz obsługujący poziomy: RAID 0/1/10/5/50/6/60.
Interfejsy	Minimum 4 porty USB; minimum 1 x port graficzny z tyłu obudowy.
Interfejsy sieciowe	1) Minimum 4 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ z modułami SFP+ SR. 2) Minimum 2 interfejsy zapewniające prędkość połączenia minimum 32Gb/s typu FC16 oraz sześć kabli światłowodowych LC-LC o długości min. 3m.
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200, dedykowana pamięć układu graficznego min. 16MB.
Porty rozszerzeń	2 gniazda PCI-Express generacji 3 lub 4 dla kart rozszerzeń.
Wentylatory	Redundantne wentylatory typu Hot-Plug.
Zasilanie	Redundantne zasilacze Hot Plug o mocy min. 800W każdy.
Bezpieczeństwo	Zintegrowany panel diagnostyczny LCD lub zestaw diod LED umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o statusie serwera. Serwer wyposażony w moduł TPM 2.0.
Zarządzanie	Serwer musi posiadać moduł zarządzający wyposażony w minimum jeden port 10/100/1000 Base-T Ethernet, pozwalający na zdalny dostęp i zarządzanie serwerem przy użyciu graficznego interfejsu Web. Moduł musi umożliwiać: 1) monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe, 2) dostęp do karty zarządzającej poprzez: a) dedykowany port RJ45 z tyłu serwera 3) dostęp do karty możliwy: a) z poziomu linii komend, b) poprzez interfejs IPMI 2.0, 4) wbudowane narzędzia diagnostyczne, 5) zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego, 6) obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie,

	7) wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników, 8) przesyłanie alertów poprzez e-mail, 9) obsługa zdalnego serwera logowania (remote syslog), 10) wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów CD/DVD, 11) monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji, 12) konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping), 13) zdalna aktualizacja oprogramowania (firmware), 14) możliwość równoczesnej obsługi przez min. 2 administratorów, 15) wsparcie dla Microsoft Active Directory, 16) obsługa TLS i SSH, 17) wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 18) Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną, posiadające dedykowany port RJ45. Całe rozwiązanie z oprogramowaniem do zdalnego zarządzania serwerem musi być produktem pochodzącym od producenta serwera oraz musi być objęte wsparciem producenta serwera.
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	1) Microsoft Windows Server 2016, 2019. 2) Red Hat Enterprise Linux (RHEL) 8. 3) SUSE Linux Enterprise Server (SLES) 15. 4) VMware ESXi 6.x, 7.x.
Certyfikaty	1) Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. 2) Oferowane urządzenie musi posiadać certyfikat CE oraz deklarację zgodności CE lub musi być oznaczony znakiem CE (oświadczenie Wykonawcy w Formularzu ofertowym).
Gwarancja	1) 60 miesięcy. 2) Usługa wsparcia technicznego musi być świadczona przez autoryzowany serwis producenta oferowanych urządzeń. 3) Uszkodzone dyski twarde pozostają własnością Zamawiającego.

II.2.3 Macierz dyskowa

Wymagane jest dostarczenie 2 szt. macierzy spełniającej poniżej opisane minimalne parametry funkcjonalne:

Cecha	Opis Wymagań
Obudowa	Obudowa do montażu w szafie rack 19” za pomocą dostarczonych dedykowanych elementów. Oferowana macierz razem z ewentualnymi półkami

	dyskowymi nie może przekroczyć rozmiaru 4U.
Kontrolery dyskowe	Macierz wyposażona w minimum 2 kontrolery pracujące w trybie active/active. Możliwość rozbudowy do co najmniej 8 kontrolerów dyskowych tworzących jedną logiczną macierz bez konieczności wymiany zaoferowanej pary kontrolerów. Rozbudowa nie może odbywać się poprzez wirtualizację (podłączanie kilku macierzy przez wirtualizator zasobów dyskowych). Kontrolery muszą komunikować się z dyskami wyłącznie protokołem NVMe. Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych.
Wydajność	Macierz w oferowanej konfiguracji w teście wydajnościowym osiągnie min. 330 000 IOPS przy następujących parametrach: - Zapełnienie macierzy – min. 80% fizycznej pojemności, - Protokół: FC, - Porty: 16G, - Read 75% - blok 8k, - Write 25% - blok 8k, - 100% Random - Read Hit Ratio – 0% - Write Hit Ratio – 0% - Latency – max 1ms - RAID 6 - Deduplikacja i kompresja - wyłączone Wymagane jest dołączenie do oferty wyników testów lub wyników symulacji z oryginalnego sizera producenta macierzy. Zamawiający ma prawo przeprowadzić test po dostawie macierzy aby sprawdzić czy dostarczone rozwiązanie osiąga deklarowane parametry wydajnościowe. Wydajność średnia nie mniejsza niż 330 000 IOPS uzyskiwana przez co najmniej 60 min testu. Ewentualny test zostanie przeprowadzony ogólnodostępnym narzędziem Vdbench.
Wymagana przestrzeń	Wymaga się dostarczenia minimum 46 dysków o pojemności 7.68TB SSD NVMe Fizyczna przestrzeń dyskowa zbudowana tylko i wyłącznie za pomocą dysków SSD NVMe/modułów NVMe o podanej pojemności. Przestrzeń użytkowa po zbudowaniu RAID 6 z 2 dyskami/modułami hot-spare lub przestrzenią hot-spare równą pojemności 2 dysków/modułów musi wynosić min 255 TiB. Dyski SSD NVMe/moduły NVMe muszą być wyposażone w podwójne, redundantne interfejsy.
Zabezpieczenia dyskami SPARE	Możliwość definiowania dysków SPARE lub odpowiedniej zapasowej przestrzeni dyskowej.
Możliwości rozbudowy macierzy	Rozbudowa oferowanej macierzy, do co najmniej 150 szt. dysków SSD NVMe/modułów NVMe, bez wymiany kontrolerów macierzowych oraz bez rozbudowy o dodatkowe kontrolery, tylko poprzez dodawanie półek i napędów dyskowych lub jeśli wymagane półek dyskowych i przełączników. Wymagany jednolity typ napędów dyskowych w ramach całej macierzy. Macierz nie może

	obsługiwać dysków HDD.
Pamięć Cache	Co najmniej 256GB pamięci cache na każdy kontroler, pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania poprzez funkcję zapisu zawartości pamięci cache na nieulotną pamięć lub posiadać podtrzymywanie bateryjne min. 48 godzin.
Dostępne interfejsy	Razem kontrolery muszą udostępnić minimum 8 interfejsów 32Gb/s FC oraz min 8 interfejsów 10G Eth. Możliwość rozbudowy o dodatkowe 8 interfejsów 16G FC oraz 4 interfejsy 25Gb/s ETH bez konieczności wymiany lub zakupu nowych kontrolerów i klastrowania z obecnie oferowanymi. Wszystkie moduły muszą posiadać wkładki optyczne. Okablowanie optyczne OM3 LC-LC dla wszystkich interfejsów oraz miedziane UTP kat 5e dla portów zarządzania o długości 5m.
Obsługiwane protokoły	Wymagana obsługa FC, NVMe over FC, iSCSI, NFS, CIFS. Wsparcie dla protokołów plikowych natywnie na macierzy i nie może odbywać się poprzez zastosowanie dodatkowego urządzenia/gateway'a.
Obsługiwane typy zabezpieczenia RAID	Kontrolery wyposażone w funkcjonalność konfiguracji poziomu RAID 6 lub równoważnego tolerującego jednoczesną awarię 2 dysków. Dodatkowo wymagana konfiguracja RAID, która pozwoli tolerować jednoczesną awarię 3 dysków bez utraty danych przy zachowaniu przestrzeni użytecznej w danej grupie RAID większej niż 50% przestrzeni surowej.
Prezentacja dysków logicznych o pojemności większej niż zajmowana przestrzeń dyskowa (ang. Thin Provisioning)	Wymagana funkcjonalność tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowych (ang. ThinProvisioning). Wymagana funkcjonalność zwrotu skasowanej przestrzeni dyskowej do puli zasobów wspólnych (ang. Space Reclamation). Wymagane dostarczenie w/w funkcjonalność na zainstalowana przestrzeń dyskową.
Zarządzanie	Zarządzanie macierzą (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu macierzy (w tym monitorowanie wydajności) oraz możliwość konfigurowania jej zasobów. Wymagana możliwość monitorowania stanu żywotności dysków SSD NVMe/modułów NVMe. Wymagana możliwość dostępu do historycznych danych wydajnościowych z poziomu GUI macierzy do co najmniej 2 lat wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożliwiającym zbieranie i przeglądanie danych historycznych. Wymagane dostarczenie w/w funkcjonalność na zainstalowaną przestrzeń dyskową.
Kopie wewnątrz	Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) w ramach macierzy do wykorzystania w celu np. wykonywania kopii zapasowych lub testów

macierzy	systemów komputerowych. Snapshoty muszą być wykonywanie w technologii ROW (Redirect On Write). Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania na całą przestrzeń dyskową i na maksymalną liczbę snapshotów obsługiwanych przez oferowany model macierzy. Tworzenie na żądanie kopii danych typu klon w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Wymagana jest możliwość kopiowania pomiędzy obszarami danych zabezpieczonych różnymi poziomami RAID. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.
Deduplikacja/kompresja	Macierz musi mieć możliwość włączenia funkcjonalności deduplikacji i kompresji danych w trybie in-line. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.
Replikacja danych	Możliwość zdalnej replikacji danych typu on-line (bez przerywania prezentacji wolumenów dyskowych) do macierzy tej samej rodziny w trybach synchroniczna oraz asynchroniczna protokołami FC lub IP. Funkcjonalność ta nie może wpływać na obciążenie serwerów podłączonych do macierzy. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.
Klaster macierzowy	Wsparcie dla technologii klastrowania macierzy dyskowych (ang. Storage Metro Cluster). Macierz musi dostarczać funkcjonalność klastra klasy "wysokiej dostępności" tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform oprogramowania i sprzętowych z wykorzystaniem synchronicznej replikacji danych po protokołach FC lub IP pomiędzy 2 macierzami. Pod użytym pojęciem "wysoka dostępność zasobów dyskowych" należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/system operacyjny/serwer) podłączonego do macierzy (macierz preferowana) w przypadku wystąpienia awarii logicznego połączenia z tą macierzą bądź awarii samej macierzy powodujących dla danego środowiska brak dostępu do zasobów macierzy preferowanej. Funkcjonalność klastra "wysokiej dostępności" pozwala na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy preferowanej na niepreferowaną w przypadku awarii macierzy preferowanej (tzw. automated failover). Wymagany jest również automatyczny failover z macierzy niepreferowanej na preferowaną. Niedopuszczalne jest osiągnięcie tej funkcjonalności przy zastosowaniu dodatkowego oprogramowania lub wirtualizatora lub gateway'a. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.
Priorytety zadań	Macierz musi posiadać możliwość zapewnienia ciągłości biznesu na oczekiwanym poziomie usług (QoS) poprzez definicję polityk QoS w oparciu o maksymalne progi wydajności IOPS i MB/s oraz minimalne progi wydajności IOPS i MB/s. Musi istnieć możliwość określenia polityk QoS na poziomie wolumenów. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.
Wspierane systemy	Wsparcie, dla co najmniej Microsoft Server Windows 2016/2019, VMware

operacyjne	6.x/7.x, Linux RedHat 7.x/8.x
Gwarancja i Serwis	Wymagane uaktualnianie firmware-u kontrolerów macierzy bez przerywania dostępu do danych. Macierz przystosowana do napraw w miejscu zainstalowania oraz wymiany elementów bez konieczności jej wyłączania. Macierz musi umożliwiać zdalne zarządzanie. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta lub autoryzowanego partnera serwisowego na terenie RP. Wymagana gwarancja i wsparcie na 5 lat w trybie 24/7 on-site. Uszkodzony dysk zostaje u Zamawiającego.
Instruktaże	Wymagane jest przeprowadzenie dedykowanych instruktaży dla 6 pracowników Zamawiającego po uruchomieniu urządzeń. Instruktaż ma na celu przekazanie wiedzy wymaganej do administrowania i zarządzania oferowaną macierzą. Instruktaż musi być przeprowadzony przez wykwalifikowanych inżynierów posiadających posiadających certyfikaty inżyniera producenta oferowanych macierzy. Instruktaż może być przeprowadzony na miejscu u Zamawiającego, bądź online. Instruktarz w wymiarze minimum 28 godzin zegarowych musi zawierać przynajmniej 40% czasu w formie warsztatów praktycznych/laboratoriów dla uczestników. Terminy instruktaży zostaną ustalone z Zamawiającym.

II.2.4 Biblioteka taśmowa

Wymagane jest dostarczenie 1 szt. biblioteki taśmowej spełniającej poniższe opisane minimalne parametry funkcjonalne:

Nazwa komponentu	Opis wymagań
Obudowa	Do zamontowania w szafie rack, maksymalnie 3U, wbudowany czytnik kodów kreskowych, redundantne zasilanie wraz z kablami zasilającymi.
Napęd	Min. 2 min. LTO9 FC z możliwością instalacji do min. 21 napędów LTO.
Interfejs	Min. 2 x FC 8Gb.
Liczba slotów	1) 40 w tym minimum pięć slotów we/wy, jeżeli licencjonowana jest liczba slotów - wymagane aktywowanie wszystkich slotów. 2) W komplecie 50 szt. taśm min. LTO9 z etykietami, 2 x taśma czyszcząca.
Dodatkowe	1) Wsparcie dla nośników LTO WORM (Write Once, Read Many), umożliwiających spełnienie norm prawnych dotyczących odpowiednio długiego przechowywania nienaruszonych danych (archiwizacja).

	2) Wsparcie dla technologii szyfrowania backupowanych danych.
Warunki gwarancji dla biblioteki taśmowej	1) Pięć lat gwarancji 2) W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych). 3) Wymagana instalacja urządzenia w szafie serwerowej rack. 4) Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta serwera – dokumenty potwierdzające załączyć do oferty.

II.2.5 Serwer kopii bezpieczeństwa

Wymagane jest dostarczenie 1 szt. serwera kopii bezpieczeństwa spełniającego poniższe opisane minimalne parametry funkcjonalne:

Nazwa komponentu	Opis wymagań
Obudowa	Maksymalnie 2U RACK 19 cali (wraz z szynami montażowymi umożliwiającymi serwisowanie serwera w szafie rack bez odłączania urządzenia). Zainstalowany z przodu obudowy panel chroniący dyski twarde przed nieuprawnionym dostępem. Serwer wyposażony w moduł TPM 2.0.
Procesor	Procesor 12-rdzeniowy klasy x86 - 64 bity, osiągający w testach SPECint_rate_base2017 wynik nie gorszy niż 165 punkty w konfiguracji dwuprocesorowej oferowanego modelu serwera.
Liczba procesorów	2
Pamięć operacyjna	1) 64GB RDIMM DDR4 2666 MT/s. 2) Płyta główna z minimum 24 slotami na pamięć i umożliwiająca. 3) instalację minimum 3TB pamięci RAM. 4) Obsługa zabezpieczeń: min. ECC
Sloty rozszerzeń	3 aktywne gniazda PCI-Express Generacji 3 lub 4
Dysk twardy	1) Obudowa serwera na minimum 12 dysków LFF 3,5'' typu Hot Swap, SAS/SATA/SSD. 2) Zainstalowane dyski: a) 12 x 12TB SAS 7.2k, b) 2 x 480GB SATA 6G M.2
Kontroler	Kontroler sprzętowy wyposażony w 4GB cache, z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę wszystkich napędów dyskowych SAS/SATA oraz obsługujący poziomy: RAID 0, 1, 10, 5, 50, 6, 60.
Interfejsy sieciowe	1) Minimum 4 porty Ethernet 100/1000 Mb/s RJ-45 ze wsparciem dla PXE. 2) Minimum 4 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ z modułami SFP+ SR. 3) Minimum 2 interfejsy zapewniające prędkość połączenia minimum 32Gb/s typu FC32 oraz cztery kable światłowodowe LC-LC o długości min. 3m.
Karta graficzna	Zintegrowana karta graficzna.
Porty	1) 4 x USB.

	2) 1x VGA. 3) Możliwość rozbudowy o port RS232.
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 500W.
Chłodzenie	Zestaw wentylatorów redundantnych.
Diagnostyka	Możliwość instalacji elektronicznego panelu diagnostycznego (lub jako rozwiązanie równoważne diody LED) z przodu serwera, pozwalającego uzyskać informacje o statusie podzespołów serwera.
Karta/moduł zarządzający	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: 1) monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe 2) dostęp do karty zarządzającej poprzez a) dedykowany port RJ45, 3) dostęp do karty możliwy : a) z poziomu przeglądarki webowej (GUI), b) poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface), 4) wbudowane narzędzia diagnostyczne, 5) zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego, 6) obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie, 7) wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników, 8) przesyłanie alertów poprzez e-mail, 9) obsługa zdalnego serwera logowania (remote syslog), 10) wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów CD/DVD, 11) monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji, 12) konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping), 13) zdalna aktualizacja oprogramowania (firmware), 14) możliwość równoczesnej obsługi przez minimum 2 administratorów, 15) wsparcie dla Microsoft Active Directory, 16) obsługa SSL i SSH, 17) wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 18) Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną, posiadające dedykowany port RJ45.
Wsparcie dla systemów operacyjnych i	5) Microsoft Windows Server 2016, 2019. 6) Red Hat Enterprise Linux (RHEL) 8. 7) SUSE Linux Enterprise Server (SLES) 15.

systemów wirtualizacyjnych	8) VMware ESXi 6.x, 7.x.
System Operacyjny	Zamawiający wymaga dostarczenia serwerowego systemu operacyjnego zgodnego z oferowanym oprogramowaniem backupowym.
Gwarancja	1) Minimum 60 - miesięczna gwarancja producenta na części, robociznę i naprawę w miejscu instalacji typu On-Site. Wszystkie dyski twarde muszą pozostać u Zamawiającego. 2) Usługa wsparcia technicznego musi być świadczona przez serwis producenta oferowanych urządzeń.
Inne	1) Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym. producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. 2) Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. 3) Oferowane urządzenie musi posiadać certyfikat CE oraz deklarację zgodności CE lub musi być oznaczony znakiem CE (oświadczenie Wykonawcy w Formularzu ofertowym). 4) Uszkodzone dyski twarde pozostają własnością Zamawiającego.

II.2.6 Deduplikator

Wymagane jest dostarczenie 1 szt. deduplikatora spełniającego poniższe opisane minimalne parametry funkcjonalne:

L.p.	Opis wymagań
1.	Urządzenie musi być przeznaczone do deduplikacji i przechowywania kopii zapasowych. Urządzenie musi spełniać wymagania wyspecyfikowane w niniejszej tabeli.
2.	Dostarczone urządzenie musi oferować przestrzeń min. 32TB netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji, wymagana skalowalność do min. 170TB netto.
3.	Oferowane urządzenie musi posiadać minimum • 2 porty SFP+ z wkładkami SFP+ SR wymagana możliwość obsługi każdym z w/w portów protokołów CIFS, NFS, deduplikacja na źródle • 2 porty FC 16Gb/s wymagana możliwość obsługi poprzez porty FC protokołów VTL oraz deduplikacja na źródle.
4.	Oferowane urządzenie musi umożliwiać jednoczesny dostęp wszystkimi poniższymi protokołami: • CIFS, NFS • zapewniającymi deduplikację na źródle – alternatywnie: OST/BOOST/CATALYST • VTL
5.	Wymagane jest dostarczenie licencji, pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, OST/BOOST/CATALYST, VTL dla maksymalnej pojemności urządzenia
6.	Oferowane pojedyncze urządzenie musi osiągać zagregowaną wydajność (dla maksymalnej konfiguracji) protokołami: NFS co najmniej 10 TB/h (dane podawane przez

	producenta) oraz co najmniej 17 TB/h z wykorzystaniem deduplikacji na źródle (dane podawane przez producenta).
7.	Urządzenie musi pozwalać na jednoczesną obsługę minimum 250 strumieni w tym jednocześnie: • zapis danych minimum 150 strumieniami • odczyt danych minimum 50 strumieniami • replikacja minimum 50 strumieniami pochodzących z różnych aplikacji oraz dowolnych protokołów (CIFS, NFS, VTL, OST/BOOST/CTALYST) oraz dowolnych interfejsów (FC, LAN) w tym samym czasie. Wymienione wartości 250 jednoczesnych strumieni dla wszystkich protokołów (czyli jednocześnie 150 dla zapisu i jednocześnie 50 strumieni dla odczytu i jednocześnie 50 strumieni dla replikacji) musi mieścić w przedziale oficjalnie rekomendowanym i wspieranym przez producenta urządzenia. Wszystkie zapisywane strumienie muszą podlegać globalnej deduplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji.
8.	Oferowane urządzenie musi mieć możliwość emulacji bibliotek taśmowych
9.	Oferowane urządzenie musi deduplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia.
10.	Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku jednak o wielkości nie większej niż 12 kB. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych co oznacza, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości, bez konieczności podejmowania czynności mających na celu ustalenie predefiniowanej długości bloków używanych do deduplikacji danych określonego typu. Deduplikacja zmiennym, dynamicznym blokiem oznacza, że wielkość każdego bloku (na jaki są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego oraz jest indywidualnie ustalana przez algorytm deduplikacji zastosowany w urządzeniu, oferowane urządzenie nie może dzielić jakiegokolwiek pojedynczego strumienia danych backupowych na bloki o ustalonej, tej samej długości.
11.	Oferowany produkt musi posiadać obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, OST/BOOST/CATALYST) przechowywanych w obrębie całego urządzenia co oznacza, że przechowywany na urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany. Wszystkie emulowane jednocześnie w obrębie urządzenia biblioteki wirtualne (VTL) oraz udziały NFS/CIFS również powinny podlegać globalnej deduplikacji – blok danych otrzymany i zapisany w wirtualnej bibliotece „A”, nie może zostać ponownie zapisany jeśli trafi do innej wirtualnej biblioteki „B” w obrębie tego samego urządzenia (to samo dotyczy udziałów NFS/CIFS). Przestrzeń składowania zdeduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych, co oznacza zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych jednocześnie protokołów dostępowych.
12.	Proces deduplikacji musi odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie zapisane jeszcze na system dyskowy urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych.
13.	Proponowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej) w celu ich późniejszej deduplikacji (wymagana deduplikacja in-line)
14.	Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane.

15.	Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje: Veeam B&R, RMAN, Microsoft SQL Server Management Studio. W przypadku współpracy z każdą z poniższych aplikacji: • Veeam B&R • RMAN (dla ORACLE) • Microsoft SQL Server Management Studio (dla Microsoft SQL) urządzenie musi umożliwiać deduplikację na źródle i przesłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN. Deduplikacja danych odbywa się na dowolnym serwerze posiadającym funkcjonalność: Media Agenta / klienta /serwera RMAN / serwera SQL . Deduplikacja w wyżej wymienionych przypadkach musi zapewniać aby z zabezpieczanych serwerów do urządzenia były transmitowane poprzez sieć LAN jedynie fragmenty danych nie znajdujące się dotychczas na urządzeniu.
16.	W przypadku przyjmowania backupów z Oracle RMAN oraz Microsoft MSSQL (przy wykorzystaniu Microsoft SQL Server Management Studio) , urządzenie musi umożliwiać deduplikację na źródle i przesłanie nowych, nieznajdujących się jeszcze na urządzeniu bloków poprzez sieć FC. Deduplikacja w wyżej wymienionych przypadkach musi zapewniać aby z serwerów do urządzenia były transmitowane poprzez sieć FC tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu.
17.	W przypadku deduplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów.
18.	Urządzenie powinno umożliwiać zaszyfrowanie przechowywanych danych, wymagane licencje umożliwiające zaszyfrowanie i przechowywanie zaszyfrowanych danych w obrębie maksymalnej pojemności oferowanego urządzenia.
19.	Urządzenie musi wspierać deduplikację na źródle poprzez sieć FC (SAN) minimum dla następujących systemów operacyjnych: • Windows • Linux (RedHat, SuSE)
20.	Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego urządzenia takiego samego typu. Konfiguracja replikacji musi być możliwa w każdym z trybów: * jeden do jednego * wiele do jednego * jeden do wielu * kaskadowej (urządzenie A replikuje dane do urządznia B, które te same dane replikuje do urządzenia C). Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu.
21.	Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji.
22.	W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.
23.	Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami – oferowane urządzenie powinno być wyposażone w mechanizm umożliwiający zarządzaniem stopnia wykorzystania pasma na potrzeby replikacji.
24.	Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu

	dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 bądź równoważnej.
25.	Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia.
26.	Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu).
27.	Urządzenie musi mieć możliwość zarządzania poprzez • Interfejs graficzny dostępny z przeglądarki internetowej • Poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell)
28.	Oprogramowanie do zarządzania musi rezydować na oferowanym na urządzeniu deduplikacyjnym.
29.	Oferowane urządzenie musi mieć możliwość sprawdzenia pakietu upgrade'ującego firmware urządzenia (GUI lub CLI), to znaczy sprawdzenia czy nowa wersja systemu nie spowoduje problemów z urządzeniem.
30.	Urządzenie musi być rozwiązaniem kompletnym, appliancem sprzętowym pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway. Oferowany typ urządzenia musi być oficjalnie dostępne w ofercie producenta przed ukazaniem się niniejszego postępowania.
31.	Gwarancja i wsparcie 60 miesięcy

II.3 Oprogramowanie systemowe i narzędziowe

II.3.1 Serwerowy system operacyjny

1. Wymagane jest dostarczenie licencji dla potrzeb 3 szt. serwerów lokalizacja nr 1 pkt. II.2.1 (minimum 6 sztuk licencji 16 core) oraz 3 szt. licencji dla serwerów lokalizacja nr 2 pkt. II.2.2 (minimum 6 sztuk licencji 16 core). W przypadku zaoferowania serwerów z sumaryczną ilością corów więcej niż 192, należy dostarczyć dodatkowe licencje.
2. Zamawiający wymaga, aby wszystkie elementy systemu oraz jego licencja pochodziły od tego samego producenta. Licencja ma umożliwiać downgrade do poprzednich wersji systemu operacyjnego oraz uprawniać do uruchamiania SSO w środowisku fizycznym i nielimitowanej ilości środowisk systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
3. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy:

L.p.	Opis wymagań
1.	Możliwość wykorzystania 320 logicznych procesorów oraz 4 TB pamięci RAM w środowisku fizycznym .
2.	Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności 64TB przez każdy wirtualny serwerowy system operacyjny.
3.	Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 7000 maszyn wirtualnych.
4.	Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet,

	bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5.	Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6.	Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7.	Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8.	Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
9.	Wbudowane wsparcie instalacji i pracy na wolumenach, które: 1) pozwalają na zmianę rozmiaru w czasie pracy systemu, 2) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, 3) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, 4) umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10.	Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11.	Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12.	Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13.	Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14.	Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15.	Graficzny interfejs użytkownika.
16.	Zlokalizowane w języku polskim, następujące elementy: 1) menu, 2) przeglądarka internetowa, 3) pomoc, 4) komunikaty systemowe.
17.	Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
18.	Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
19.	Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
20.	Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).
21.	Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: 1) podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, 2) usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, pozwalające na zarządzanie zasobami w sieci (użytkownicy,

	komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: a) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, b) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, c) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, 3) zdalna dystrybucja oprogramowania na stacje robocze, 4) praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, 5) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: 6) dystrybucja certyfikatów poprzez http , 7) konsolidacja CA dla wielu lasów domeny, 8) automatyczne rejestrowanie certyfikatów pomiędzy różnymi lasami domen. 9) szyfrowanie plików i folderów, 10) szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), 11) możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów, 12) serwis udostępniania stron WWW. 13) wsparcie dla protokołu IP w wersji 6 (IPv6), 14) wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, 15) wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtulne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji zapewniające wsparcie dla: a) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, b) obsługi ramek typu jumbo frames dla maszyn wirtualnych, c) obsługi 4-KB sektorów dysków, d) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, 16) możliwość kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), 17) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
22.	Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).

23.	Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
24.	Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
25.	Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

II.3.2 Oprogramowanie wirtualizacyjne

1. Wymagane jest dostarczenie licencji dla potrzeb 3 szt. serwerów lokalizacja nr 1 pkt II.2.1 oraz 3 szt. serwerów lokalizacja nr 2 pkt II.2.2, zgodnie z licencjonowanie oferowanego oprogramowania wraz z centralną konsolą zarządzającą.
2. Minimalne wymagania na oprogramowanie do wirtualizacji serwerów:

L.p.	Opis wymagań
1.	Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych.
2.	Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
3.	Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości 62 TB.
4.	Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia 24 TB pamięci operacyjnej RAM.
5.	Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.
6.	Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe.
7.	Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 20 portów USB.
8.	Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 4 GB pamięci graficznej.
9.	Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
10.	Rozwiązanie musi w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
11.	Rozwiązanie musi wspierać następujące systemy operacyjne: 8/10, Windows Server, Amazon Linux 2, macOS, OS X, Asianux, Ubuntu, CentOS, NeoKylin, CoreOS, Debian, FreeBSD, Oracle Linux, RHEL, SUSE, Photon OS.
12.	Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
13.	Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
14.	Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów

	dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
15.	System musi posiadać funkcjonalność wirtualnego przełącznika sieciowego umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny musi mieć możliwość konfiguracji do 4000 portów.
16.	Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
17.	Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).
18.	Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Wsparcie techniczne musi być świadczone bezpośrednio przez producenta oprogramowania. Licencjonowanie nie może odbywać się w trybie OEM.
19.	Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności Microsoft Active Directory, Open LDAP.
20.	Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
21.	Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych pomiędzy różnymi systemami pamięci masowych.
22.	Rozwiązanie musi zawierać funkcjonalność pozwalającą na ominięcie testów inicjalizacyjnych sprzętu fizycznego w celu szybkiego startu wirtualizatora.
23.	Rozwiązanie musi zawierać możliwość zabezpieczania maszyn wirtualnych przez rozwiązania antywirusowe firm trzecich bez konieczności instalacji agenta wewnątrz maszyny wirtualnej.
24.	Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy, bez jakiegokolwiek przestoju i bez utraty danych, pomiędzy serwerami fizycznymi, niezależnie od dostępności współdzielonej przestrzeni dyskowej.
25.	Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy, bez jakiegokolwiek przestoju i bez utraty danych, pomiędzy zasobami dyskowymi, niezależnie od dostępności współdzielonej przestrzeni dyskowej.
26.	Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy, bez jakiegokolwiek przestoju i bez utraty danych, jednocześnie między serwerami fizycznymi oraz zasobami dyskowymi, niezależnie od dostępności współdzielonej przestrzeni dyskowej.
27.	Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA), aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym. Rozwiązanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci.
28.	Rozwiązanie musi zapewniać wsparcie dla wirtualizacji zagnieżdżonej, w szczególności w zakresie możliwości zastosowania wszystkich funkcjonalności w tym Hyper-V systemu

	Windows Server na maszynie wirtualnej.
29.	Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej.
30.	Oprogramowanie do wirtualizacji musi zapewniać mechanizm takiego zabezpieczenia wybranych przez administratora wirtualnych maszyn, aby w przypadku awarii lub niedostępności serwera fizycznego maszyny, które na nim pracowały, były bezprzerwowo dostępne na innym serwerze z zainstalowanym oprogramowaniem wirtualizacyjnym. Mechanizm ten umożliwia zabezpieczenie maszyn wirtualnych wyposażonych w minimum 2 wirtualne procesory /8 wirtualnych procesorów.
31.	Rozwiązanie musi umożliwiać automatyczne równoważenie obciążenia CPU/MEM serwerów fizycznych pracujących jako platforma dla infrastruktury wirtualnej.
32.	Rozwiązanie musi mieć możliwość oszczędzania energii elektrycznej poprzez automatyczne wyłączenie wskazanych serwerów fizycznych w przypadku braku obciążenia generowanego przez wirtualne maszyny i automatycznego ich włączenia w sytuacji wzrostu obciążenia.
33.	Rozwiązanie musi mieć możliwość automatycznego równoważenia obciążenia fizycznych zasobów dyskowych poprzez przenoszenie zwirtualizowanych dysków pracujących maszyn wirtualnych pomiędzy fizycznymi zasobami dyskowymi.
34.	Oprogramowanie do wirtualizacji musi zapewniać mechanizm pozwalający tworzyć profil (szablon konfiguracji) wybranego serwera a następnie instalować ten profil/konfigurację na innych serwerach lub sprawdzać zgodność konfiguracji pomiędzy zdefiniowanym wcześniej profilem a wskazanym serwerem fizycznym.
35.	Rozwiązanie musi mieć możliwość uruchamiania fizycznych serwerów wchodzących w skład infrastruktury z obrazu udostępnionego poprzez protokół PXE.
36.	Rozwiązanie musi umożliwiać szyfrowanie danych oraz dysków wirtualnych maszyn.
37.	Rozwiązanie natywnie wspiera technologię Nvidia vGPU.
38.	Zaoferowane oprogramowanie musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowanego wirtualnego urządzenia dedykowanego dla poszczególnych maszyn wirtualnych.
39.	Zaoferowane oprogramowanie musi wspierać funkcjonalność bezpośredniego tworzenia kontenerów oraz klastrów Kubernetes na hiperwizorze (warstwie wirtualizatora) za pomocą dostarczonej konsoli zarządzającej Kubernetes (Kubectl) – jeśli włączenie tej funkcji w warstwie wirtualizatora może wymagać dodatkowej licencji/subskrypcji, Zamawiający nie wymaga tej licencji w przedmiotowym postepowaniu.
40.	Oprogramowanie musi posiadać centralną konsolę graficzną do zarządzania wieloma maszynami wirtualnymi oraz ich zasobami pracującymi na wielu serwerach fizycznych: 1) globalne zarządzanie kontrolą dostępu do serwerów i maszyn wirtualnych 2) wykonywanie automatycznych bądź manualnych zadań w celu optymalizacji infrastruktury dla maszyn wirtualnych. 3) widok całego systemu i zbioru maszyn wirtualnych. Mapy Infrastruktury. 4) możliwość monitorowania dostępności i wydajności maszyn wirtualnych 5) możliwość raportowania dostępności i wydajności maszyn wirtualnych 6) funkcje ochrony dostępu zintegrowane z mechanizmem uwierzytelniania Windows 7) planowanie zadań i ustawianie znaczników alarmów w celu generowania automatycznych powiadomień o statusie serwerów lub maszyn wirtualnych

	8) tworzenie obrazów maszyn wirtualnych 9) klonowanie maszyn wirtualnych 10) wykonywanie wielu kopii migawkowych (snapshoot) w każdym momencie pracy maszyny wirtualnej oraz możliwość powrotu do jej stanu z każdego momentu zrobienia kopii
41.	Konsola administracyjna powinna umożliwiać monitorowanie i zarządzanie nowym środowiskiem maszyn wirtualnych, przy jednoczesnej integracji z już istniejącą infrastrukturą VMware vCenter Standard 7.0 u Zamawiającego. Integracja powinna funkcjonować w ramach tej samej domeny Single Sign-On (np. za pomocą mechanizmu Enhanced Linked Mode). Co oznacza, że będzie można zalogować się do połączonych systemów jednocześnie za pomocą jednej nazwy użytkownika i hasła, będzie można przeglądać spis wszystkich połączonych maszyn wirtualnych, nadawać role, uprawnienia, znaczniki w połączonych systemach oraz migrować maszyny wirtualne.
42.	Wymaga się dostarczenia opisanego oprogramowania z okresem wsparcia na 60 miesięcy.

II.3.3 Oprogramowanie backupowe

Minimalne wymagania na oprogramowanie do wykonywania kopii zapasowych całości dostarczanego w/w środowiska:

L.p.	Opis wymagań
1.	Oprogramowanie musi umożliwiać backup nieograniczonej ilości maszyn wirtualnych z dostarczanych 6 serwerów 2 procesorowych. Wymagane wsparcie 5 lat.
2.	Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2012, 2012 R2 i 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.
3.	Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
4.	Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.
5.	Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V.
6.	Oprogramowanie musi zapewniać tworzenie kopii zapasowych z serwerów plikowych opartych o Windows i Linux.
7.	Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.
8.	Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków.
9.	Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny i przyrostowy.
10.	Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.
11.	Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata

	bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
12.	Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
13.	Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time).
14.	Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API.
15.	Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.
16.	Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji.
17.	Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania.
18.	Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
19.	Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.
20.	Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora.
21.	Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
22.	Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn.
23.	Oprogramowanie musi posiadać wsparcie dla NDMP.
24.	Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).
25.	Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
26.	Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu.
27.	Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą.
28.	Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik.
29.	Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli.
30.	Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing).
31.	Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre.

32.	Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.
33.	Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny.
34.	Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
35.	Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików: 1) **Linux:** ext2, ext3, ext4, ReiserFS, XFS, 2) **Solaris** ZFS, UFS, 3) **Windows** NTFS, FAT32, ReFS,
36.	Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
37.	Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD, Microsoft System Objects, certyfikaty CA oraz elementy AD Sites.
38.	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects").
39.	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat.
40.	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. Opcja odtworzenia elementów, witryn, uprawnień.
41.	Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
42.	Oprogramowanie musi pozwalać na zaprezentowanie baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego.
43.	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN.
44.	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA.
45.	Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
46.	Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku.
47.	Oprogramowanie musi umożliwiać integrację oraz współpracę z deduplikatorem sprzętowym w procesie tworzenia i odzyskiwania kopii zapasowych. .

II.3.4 System ochrony aplikacji webowych oraz XML

System ochrony aplikacji webowych oraz XML będzie wykrywał i blokował ataki na poziomie warstwy aplikacyjnej HTTP/HTTPS. System powinien zostać dostarczony w postaci platformy instalowanej w środowisku wirtualnym VMware, Microsoft Hyper-V, Amazon Web Services (AWS), Microsoft Azure.

Lp.	Opis	Minimalne wymagania
1	**Architektura systemu**	a) Dla zapewnienia wysokiej sprawności i skuteczności działania wymaganym jest aby elementy systemu pracowały w oparciu o dedykowane oprogramowanie, wzmocnione z punktu widzenia bezpieczeństwa. b) Dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje podstawowe oraz zastosowane w nich technologie pochodziły od jednego producenta. Nie dopuszcza się aby elementy funkcji podstawowych zastosowanych w systemie były opracowane przez firmy trzecie. c) Musi istnieć możliwość implementacji systemu w trybach: „reverse proxy” lub „transparent” d) Produkt nie może posiadać ograniczeń co do ilości chronionych aplikacji web. e) Powinna istnieć możliwość zdefiniowania co najmniej 4 domen administracyjnych (ról), w których poszczególni administratorzy zarządzają określonymi funkcjami systemu. f) System powinien mieć możliwość pracy w konfiguracji HA (High Availability) w trybie Active-Passive i Active-Active.
2	**Parametry fizyczne systemu**	a) System realizujący funkcje podstawowe musi obsługiwać minimum: • 4 interfejsy sieciowe • Ilość wirtualnych procesorów vCPU: 4 • Ilość wirtualnej pamięci vRAM: 16 • Ilość wirtualnej powierzchni dyskowej vHDD: 1TB
3	**Parametry wydajnościowe**	a) Przepustowość dla ruchu HTTP z obsługą funkcji Web Application Firewall – min. 500 Mbps
4	**Podstawowe funkcje systemu**	System musi realizować co najmniej poniższe funkcje: a) Obsługa protokołów: - http 1.1, http 2.0. a) Automatyczne tworzenie profili ochronnych aplikacji na bazie zaobserwowanego ruchu. Możliwość wyboru trybu wymuszania wyuczonego schematu bez konieczności akceptacji przez administratora. b) Automatyczne tworzenie profilu ochrony przed botami na bazie zaobserwowanego ruchu użytkowników c) Podział obciążenia na kilkanaście serwerów (loadbalancing) z mechanizmami weryfikacji stanu pracy serwerów. Wsparcie dla różnych mechanizmów podziału obciążenia typu „losowo”, „najmniejsza liczba połączeń”. d) Wsparcie dla mechanizmów „session persistence” dla co najmniej „cookie” e) Terminowanie połączeń SSL dla wybranych chronionych

		serwisów. Wsparcie dla TLS 1.1, TLS 1.2. TLS 1.3. f) Możliwość analizy ruchu do aplikacji po protokołach HTTP/HTTPS w oparciu o zaimplementowane polityki bezpieczeństwa. g) Ochrona aplikacji www przed takimi zagrożeniami jak: • SQL and OS Command Injection. • Cross Site Scripting (XSS). • Cross Site Request Forgery. • Outbound Data Leakage. • HTTP Request Smuggling. • Buffer Overflow. • Encoding Attacks. • Cookie Tampering / Poisoning. • Session Hijacking. • Forceful Browsing /Directory Traversal. • Ochrona przed innymi zagrożeniami specyfikowanymi przez listę OWASP. • DoS w warstwie aplikacji. • Ochrona przed atakami typu Brute force. • Ochrona przed atakami clickjacking. • Ochrona przed credential stuffing. h) Mechanizmy ochrony przed wyciekiem informacji poufnych. i) Filtrowanie ruchu do aplikacji w oparciu o geo-lokalizację. j) Analiza komunikacji w oparciu o bazy reputacyjne adresów IP, dostarczane przez producenta rozwiązania. k) Wsparcie dla ochrony HTTP/1.1 i HTTP/2 oraz offload dla HTTP/1.1 i HTTP/2 w trybie pracy reverse proxy. l) Wsparcie dla ochrony cookie m) Content routing na bazie parametrów http oraz certyfikatów X.509. n) Ochrona przed Web Scraping. o) Bezpieczne udostępnianie (publikacja) aplikacji OWA oraz SharePoint w Internecie z uwierzytelnieniem NTLM oraz Kerberos p) Wsparcie dla aplikacji wykorzystujących AJAX oraz JSON, XML, AMF3. q) Ochrona przed atakami typu SLOW (Slowloris i podobne). r) Możliwość selektywnego wyłączania blokowania ataków dla sygnatur oraz obszarów aplikacji. Dodanie wyjątków dla sygnatur na podstawie wielu parametrów: • Metoda HTTP. • Parameter http. • Host. • Url. • Cookie. s) Funkcja korzystania ze źródłowego adresu IP przekazywanego w nagłówku http „X-Forwared-For”. t) Możliwość konfigurowania własnych stron z informacjami o błędzie w reakcji na wykryty incydent. u) Sprawdzanie sekwencji otwieranych stron. v) Sprawdzanie pól w nagłówkach http oraz samym protokole. Sprawdzanie długości payload’u HTML.

		w) Wsparcie dla walidacji i blokowania niepoprawnego formatu JSON i XML. x) Przydzielanie różnych certyfikatów dla różnych nazw domenowych. y) Ochrona przed atakami MiTB (Man-in-the-Browser)
5	**Wymagane funkcje dodatkowe**	a) Kontrola antywirusowa dla komunikacji http realizowana na firewall'u aplikacyjnym WAF lub w zewnętrznym systemie. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji. b) Możliwość integracji z usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. c) Skaner aplikacji WWW realizowany bezpośrednio na firewall'u aplikacyjnym lub zewnętrznym systemie (w przypadku zewnętrznego systemu skanującego – musi istnieć możliwość importu wyników skanowania do systemu WAF oraz na tej podstawie konfiguracji polityk ochrony). W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji. d) Ochrona przed podmianą strony WWW realizowana bezpośrednio na firewall'u aplikacyjnym WAF lub zewnętrznym systemie. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji. a) Domyślne szablony ochrony WWW. b) Wsparcie dla CAPTCHA lub Real Browser Enforcement do weryfikacji użytkowników. c) Budowa rankingu lub określanie poziomu zagrożenia dla ruchu (użytkownika w Internecie) z możliwością określenia progów dla poszczególnych akcji: logowanie, blokowanie, kwarantanna czasowa.
6	**Zarządzanie**	a) Dostarczony system musi umożliwiać lokalne zarządzanie z wykorzystaniem protokołów HTTPS, SSH. b) Element systemu pełniący funkcję Web Application Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: debug, packet capture lub inne przechwytujące pakiety w surowej postaci (np. tcpdump). c) Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.
7	**Logowanie i Raportowanie**	a) System musi zapewniać lokalne logowanie oraz raportowanie - w oparciu o zestaw predefiniowanych wzorców raportów. b) Możliwość logowania do zewnętrznego serwera syslog i SIEM. c) Obsługa powiadomień o zdarzeniach systemowych oraz incydentach bezpieczeństwa mailem. d) Powiadomienia o zdarzeniach systemowych oraz incydentach bezpieczeństwa za pośrednictwem trapów SNMP.
8	**Certyfikaty**	a) Z punktu widzenia jakości i skuteczności rozwiązania koniecznym jest przedstawienie wyników testów niezależnych organizacji, np. NSS Labs, ICSA Labs lub równoważnego.
9	**Sygnatury, subskrypcje**	a) Bazy sygnatur wykorzystywane przez funkcje ochronne powinny być systematycznie aktualizowane zgodnie ze

		zdefiniowanych harmonogramem. b) W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych i serwisów. Powinny one obejmować: sygnatury i profile ochrony dla aplikacji www oraz bazy reputacyjne adresów IP na okres 60 miesięcy.

II.4 Dostawa i wdrożenie Regionalnego Systemu Informatycznego RSI

II.4.1 Ogólna architektura funkcjonalna projektu ZeZ

W odniesieniu do poszczególnych e-usług w zależności od uwarunkowań implementacji wymagany jest następujący poniżej omówiony zakres prac.

Dla e-usług i kluczowych funkcjonalności dla Projektu ZeZ założono i przyjęto udział obecnych i planowanych rozwiązań zarówno na poziomie centralnym, warstwy regionalnej na poziomie Województwa Zachodniopomorskiego oraz warstwy lokalnej na poziomie Partnerów Projektu / podmiotów leczniczych.

1) Poziom centralny, w tym w szczególności P1 w zakresie:
   a) Internetowe Konto Pacjenta (IKP),
   b) rejestr Elektroniczna Dokumentacja Medyczna (EDM) w obecnym i dalszych rozszerzeniach zakresu stosowania dla kolejnych dokumentów medycznych (od 25 kwietnia 2020 r. EDM stanowią również opisy badań diagnostycznych innych niż laboratoryjne, a od 25 kwietnia 2021 r. są to także wyniki badań laboratoryjnych wraz z opisem),
   c) Zdarzenia Medyczne,
   d) zgody Pacjenta,
   e) System Elektronicznej Rejestracji
   f) kolejne e-usługi planowane do uruchomienia w przyszłości, m.in. e-Wizyty, zamawianie e-Recept, recepta transgraniczna
   g) uwierzytelnianie z wykorzystaniem Węzła Krajowego Identyfikacji Elektronicznej poprzez: Profil zaufany (PZ), e-dowód oraz mojeID - przy pomocy banku lub innego dostawcy tożsamości.
2) Warstwa regionalna w zakresie:

Platforma regionalna o następującym zakresie funkcjonalnym:

   a) Regionalne Repozytorium EDM,
   b) Portal Projektu ZeZ,
   c) Systemy analityczne:
      1. System Analiz Zarządczych
      2. System Analiz Sprawozdawczych
      3. Platforma zakupowa SPZOZ/Grupowe zamówienia

Warstwa regionalna wspiera i uczestniczy w świadczeniu usług oraz zapewnia udostępnianie EDM dla pacjenta i innym podmiotom leczniczym.

3) Warstwa lokalna na poziomie Partnera:
   a) integracja z krajowym Systemem Elektronicznej Rejestracji na Platformie P1,

b) e-Rejestracja lokalna przez stronę www w powiązaniu z e-Rejestracją centralną (SER)
c) lokalne repozytorium EDM,
d) integracja z Regionalnym Repozytorium EDM,
e) EDM i zdarzenia medyczne dla pacjenta (poprzez IKP)
f) EDM i zdarzenia medyczne dla lekarza
g) przesyłanie indeksów EDM oraz danych o zdarzeniach medycznych do P1,
h) integracja z P1 w zakresie odczytu i zapisu zgód pacjenta

Warstwa lokalna świadczy usługi dla pacjentów z zastosowaniem poziomu centralnego oraz warstwy regionalnej.

Rejestr oraz repozytorium EDM wskazane na poziomie centralnym i w warstwach regionalnej i lokalnej, rozumiane są następująco:

- źródłem danych dla dokumentacji EDM (Document Source) jest system części białej (HIS, LIS, RIS) w podmiocie leczniczym,
- dokumenty EDM są składowane i archiwizowane w repozytorium lokalnym podmiotu leczniczego;
- informacje opisujące elektroniczną dokumentację medyczną EDM (metadane, indeksy) oraz wskazujące gdzie przechowywana jest właściwa dokumentacja zawarte są w Rejestrze EDM w P1 w ramach Krajowej Domeny (IHE XDS.b),
- informacje do Rejestru EDM są przekazywane bezpośrednio przez podmiot leczniczy,
- **Regionalne Repozytorium EDM jest zasilane dokumentami EDM z lokalnego repozytorium EDM podmiotu leczniczego Partnera Projektu ZeZ;**
  - **Regionalne Repozytorium EDM zostanie przygotowane w taki sposób, że inne podmioty lecznicze niebędące Partnerami Projektu będą miały możliwość przystąpienia do platformy ZeZ w celu przechowywania kopi swoich dokumentów medycznych przeznaczonych do udostępniania na platformie P1. Wykonawca przygotuje i przekaże w ramach wdrożenia instrukcję oraz przeszkoli personel Zamawiającego w zakresie tworzenia dedykowanych repozytoriów dla przyszłych Partnerów.**

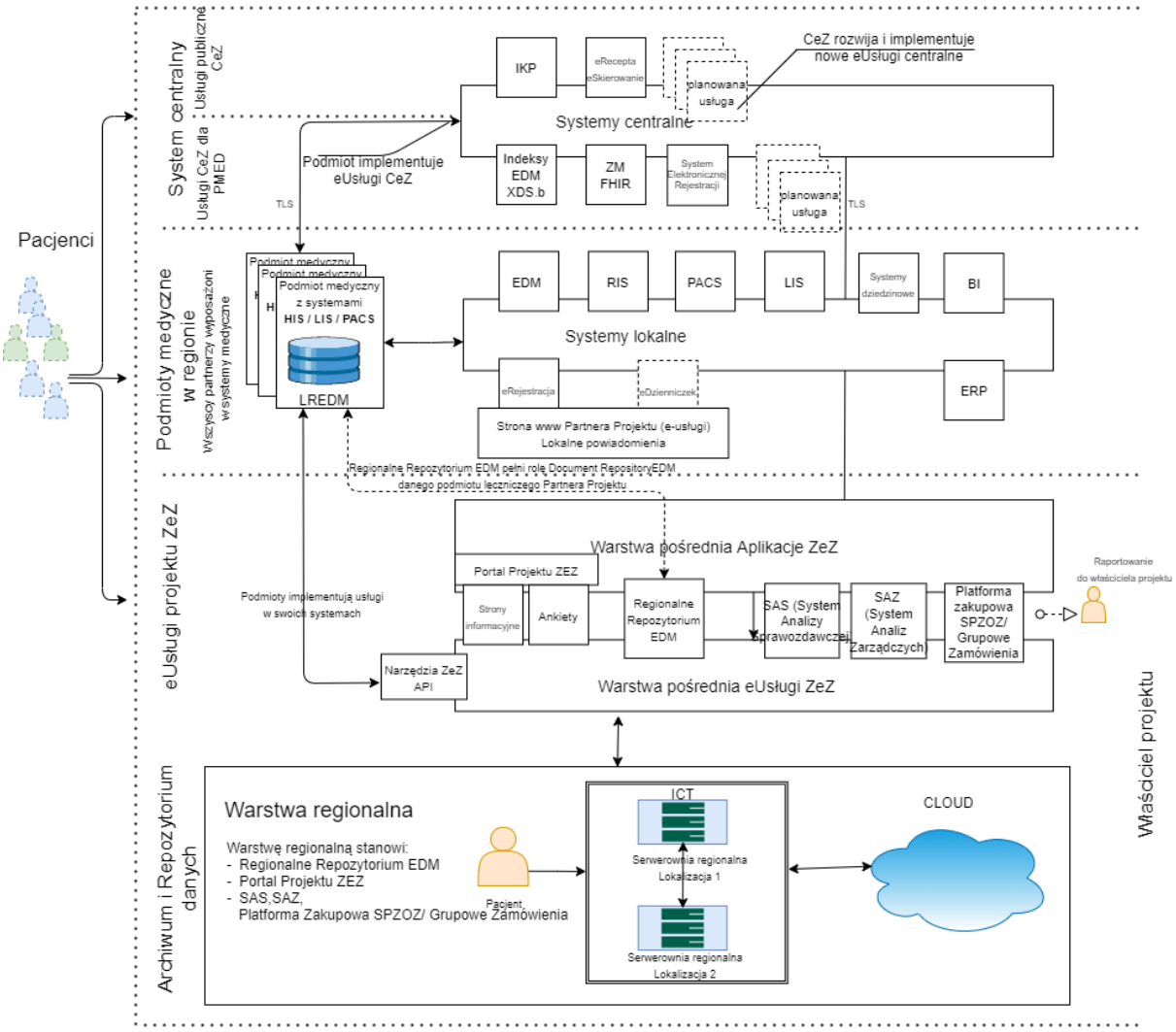
- **Regionalne Repozytorium pełni rolę Document Repository EDM danego podmiotu leczniczego Partnera Projektu;**
- **kierowanie zapytań o dokumentację EDM z wykorzystaniem rejestru EDM w P1 oraz zgody pacjenta od innych świadczeniodawców odbywa się do Regionalnego Repozytorium,**
- **udostępnianie EDM dla zewnętrznych użytkowników (pacjentów i pracowników medycznych) odbywa się z Regionalnego Repozytorium EDM poprzez Internetowe Konto Pacjenta w systemie P1 (dla pacjentów) lub poprzez systemy dziedzinowe, w tym HIS (dla pracowników medycznych).**

Uwagi:
- warstwa regionalna nie prowadzi rejestru (indeksów) EDM. Indeksowanie EDM w P1 prowadzone jest przez Partnera Projektu ZeZ;
- Indeks Pacjenta nie jest wymagany na poziomie regionalnym;

- **raportowanie/przekazywanie informacji o Zdarzeniach Medycznych będzie realizowane przez podmiot leczniczy lokalnie ze wskazaniem Regionalnego Repozytorium EDM jako Document Repository EDM;**
- **wdrożenie Regionalnego Repozytorium EDM jako repozytorium uczestniczącego w wymianie i udostępnianiu dokumentacji EDM nie wyklucza możliwości przełączenia i wskazania jako Dokument Repository w rejestrze EDM P1 repozytorium lokalnego Partnera Projektu. Zapewnia redundantność zapisu danych EDM oraz jedno miejsce w Systemie udostępniania danych;**
- podmiot leczniczy wdraża e-Rejestrację lokalną, do której dostęp zapewniony będzie poprzez stronę (witrynę) www podmiotu leczniczego;
- systemy oprogramowania danego podmiotu zostaną zintegrowane z Systemem Elektronicznej Rejestracji na Platformie P1.

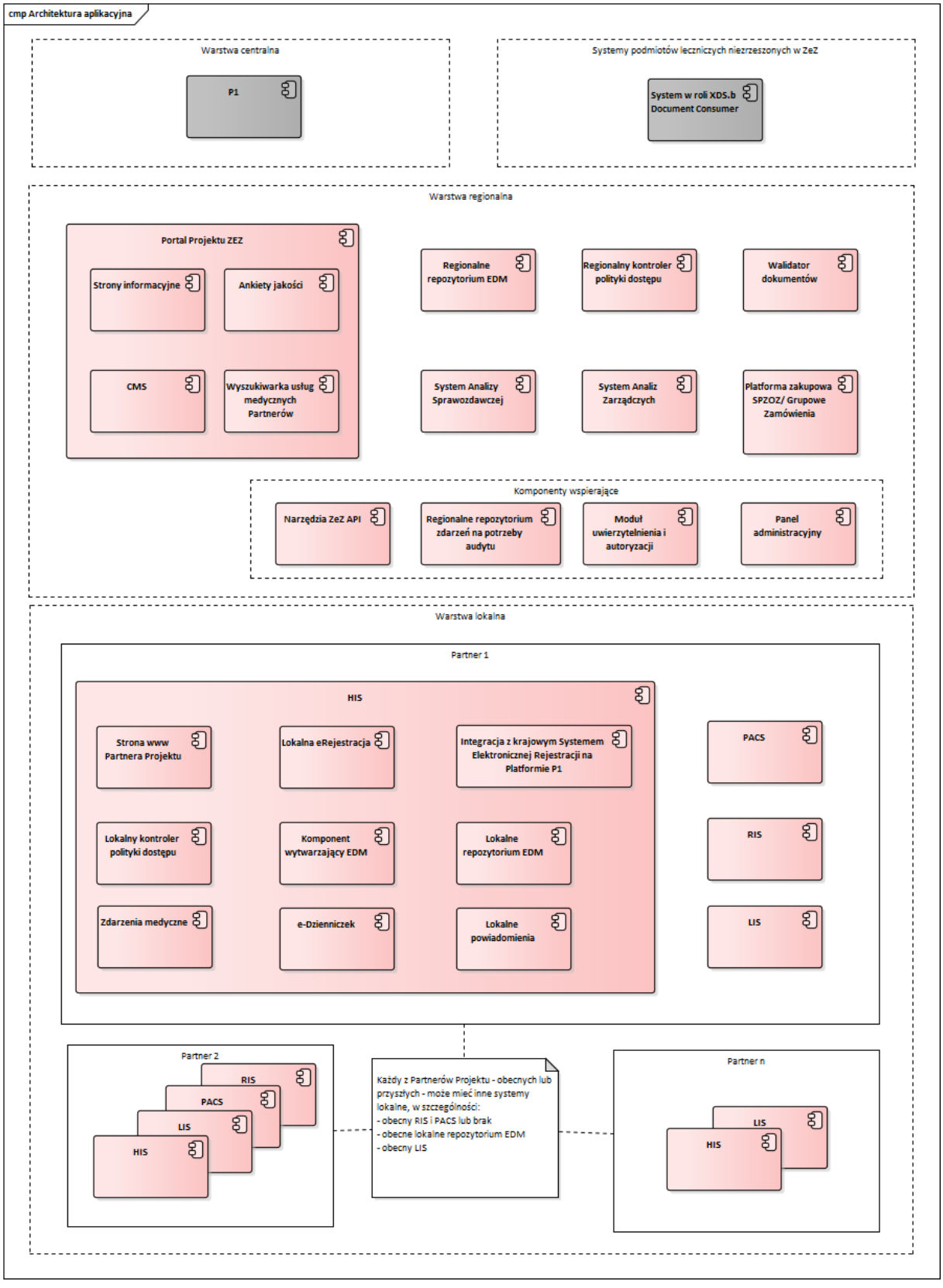
II.4.2 Architektura logiczna projektu „Zachodniopomorskie e-Zdrowie”

Schemat 1. Ogólny model koncepcyjny Projektu „Zachodniopomorskie e-Zdrowie”



II.4.3 Model architektury aplikacyjnej

Schemat 2. Architektura aplikacyjna ZEZ



II.4.4 Dostępność dostarczanego rozwiązania

Regionalny System Informatyczny RSI działa w trybie 24 godzinnym przez wszystkie dni w roku z dostępnością, co najmniej na poziomie 99% w skali miesiąca dla e-usług. System nie jest dostępny, gdy występuje sytuacja uniemożliwiająca wykorzystanie którejś z jego funkcji z przyczyn leżących wewnątrz Systemu (np. awarii, spadku przepustowości Systemu i wynikającego stąd przeciążenia Systemu, awarii infrastruktury). Planowane prace serwisowe (tzw. down time) odbywają się wyłącznie w dni robocze w godzinach od 13:00 do 18:00. W ciągu jednego miesiąca mogą odbyć się maksymalnie dwie takie przerwy. Czas planowych prac serwisowych (down time) nie jest liczony jako niedostępność i musi być uzgodniony z Zamawiającym i przez niego zaakceptowanym w formie pisemnej (mailowej lub w formie pisma).

II.4.5 Regionalny System Informatyczny

II.4.5.1 Wymagania ogólne

1. Wykonawca musi wykonać i dostarczyć Zamawiającemu Regionalny System Informatyczny składający się z:
   1) Regionalnego Repozytorium EDM (pełniące funkcję Document Repository dla Partnerów Projektu) wraz z przygotowaniem *Dokumentacji integracyjnej oprogramowania warstwy lokalnej z warstwą regionalną*
   2) Portal Projektu ZeZ zawierający m.in. katalog wszystkich e-usług świadczonych przez jednostki ochrony zdrowia (Partnerów Projektu), wdrożonych w Lokalnych Portalach Pacjenta, w ramach Projektu „Zachodniopomorskie e-Zdrowie”,
2. Warstwa regionalna świadczy samodzielnie usługę dla pacjentów (informacyjną związaną z Portalem Projektu ZeZ). Warstwa regionalna wspiera i uczestniczy w świadczeniu usług oraz zapewnia ciągłość udostępniania EDM.

II.4.5.2 Struktura repozytoriów EDM (repozytorium regionalne oraz lokalne)

Architektura systemu Zachodniopomorskie e-Zdrowie zaprezentowana jest szeroko w dokumencie *Model realizacyjny ZeZ* oraz w wersji skróconej w dokumencie stanowiącym załącznik nr … do SWZ. Rozdział II.4.1 zawiera natomiast skrócony opis w kontekście założonej logiki procesów systemu ZeZ.

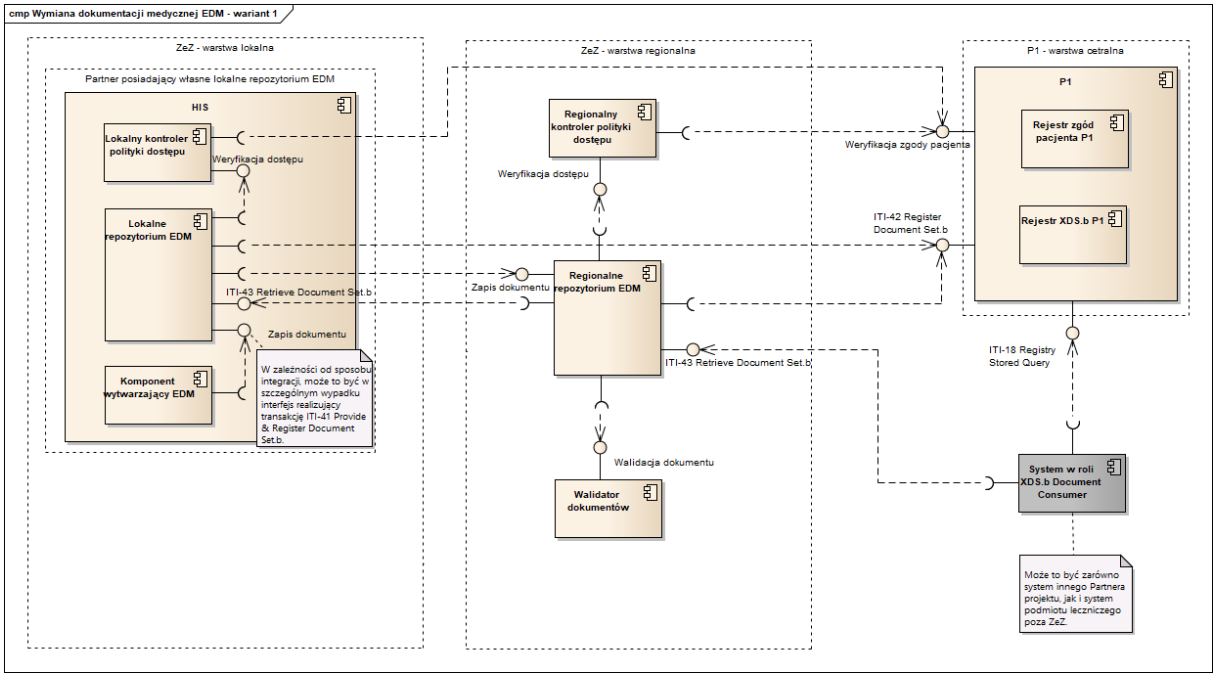
Poniżej przedstawione zostały kluczowe informacje istotne z punktu widzenia sposobu implementacji dostępu do repozytorium dokumentacji EDM.

Podstawowym założeniem Projektu jest wdrożenie i użytkowanie przez podmiot leczniczy - Partnera w Projekcie ZeZ dwóch repozytoriów: lokalnego i regionalnego.

1. Repozytorium lokalne EDM (LREDM) – jest to repozytorium podstawowe - *primary*.
   Założenia:
   - repozytorium jest wdrożone i użytkowane w systemie dziedzinowym HIS lokalnym;
   - repozytorium lokalne zasilane jest na bieżąco danymi - dokumentami EDM z systemów dziedzinowych: HIS, LIS, PACS/RIS i innych wymaganych w przyszłości, w zależności od listy definiowanych przez resort zdrowia dokumentów EDM;
   - użytkowanie repozytorium wymaga alokowania lokalnych zasobów obliczeniowych: serwer bazy danych, macierz dyskowa, oraz dla bezpieczeństwa danych system archiwizacji i backupu;
   - możliwe są również – jednak nie implementowane w chwili obecnej w Projekcie ZeZ – rozwiązania typu IaaS lub PaaS.
2. Repozytorium regionalne EDM (RREDM) – jest to repozytorium - *secondary*.
   Założenia:
   - repozytorium to jest zasilane danymi z repozytorium lokalnego w trybie replikacji on-line;
   - wdrożenie i użytkowanie repozytorium w oparciu o zasoby infrastrukturalne dostępne w warstwie regionalnej.
3. Kluczowe założenia architektury:
   - Regionalne Repozytorium EDM przechowuje kopię dokumentów medycznych, które są zaindeksowane i przeznaczone do udostępniania na platformie P1 pełniąc rolę Dokument Repository
   - wymiana oraz udostępnianie dokumentacji EDM z innymi podmiotami leczniczymi jak również jej udostępnianie odbywa się jedynie z wykorzystaniem Repozytorium Regionalnego - zasobów warstwy regionalnej, przy czym dostęp do własnej dokumentacji pacjent uzyska jedynie poprzez IKP;
   - rozwiązanie gwarantuje zwiększony poziom dostępności dokumentacji EDM, zwiększoną odporność systemu na awarie;
   - podmiot leczniczy jest właścicielem dokumentacji EDM (kustoszem w rozumieniu Dokumentacji integracyjnej EDM wydanej CeZ) – rozwiązanie gwarantuje możliwość ew. przyszłej migracji repozytorium do planowanej chmury publicznej lub innego systemu bez utraty integralności danych.

II.4.5.2.1 Architektura aplikacyjna obszaru wymiany dokumentacji medycznej EDM

Poniższy diagram obrazuje komponenty aplikacyjne zaangażowane w realizację obszaru wraz z wykorzystywanymi w tym celu operacjami.



II.4.5.3 Regionalne Repozytorium EDM

1. Regionalne Repozytorium EDM ma mieć możliwość przechowywania kopii dokumentów medycznych, które są zaindeksowane i przeznaczone do udostępniania na platformie P1 pełniąc rolę Dokument Repository.
2. Regionalne Repozytorium ma być zasilane danymi z repozytorium lokalnego w trybie replikacji on-line.
3. Dla każdego z Podmiotów Leczniczych uczestniczących w Projekcie ZeZ Wykonawca utworzy niezależną przestrzeń w Regionalnym Repozytorium EDM. Ilość repozytoriów oraz konieczna przestrzeń dla każdego z Partnerów zostanie ustalona na etapie Analizy Przedwdrożeniowej.
4. Repozytorium zostanie przygotowane w taki sposób, że inne podmioty lecznicze niebędące Partnerami Projektu będą miały możliwość przystąpienia do platformy ZeZ w celu przechowywania kopi swoich zaindeksowanych dokumentów medycznych przeznaczonych do udostępniania na platformie P1. Wykonawcy przygotuje i przekaże w ramach wdrożenia instrukcję oraz przeszkoli personel Zamawiającego w zakresie tworzenia dedykowanych repozytoriów dla przyszłych Partnerów.
5. Wymiana oraz udostępnianie dokumentacji EDM (pacjentowi lub pracownikowi medycznemu) z innymi podmiotami leczniczymi jak również jej udostępnianie odbywa się jedynie z wykorzystaniem Regionalnego Repozytorium EDM - zasobów warstwy regionalnej, przy czym dostęp do własnej dokumentacji pacjent uzyska jedynie poprzez IKP
6. Moduł Regionalnego Repozytorium EDM musi spełniać poniższe wymagania:

L.p.	Opis wymagań
1.	Umożliwienie zapisu Dokumentów medycznych w postaci elektronicznej, w szczególności: a. zgodnych z PIK HL7 CDA b. zgodnych z inną implementacją HL7 CDA c. zgodnych z DICOM d. w innych formatach.
2.	Umożliwienie zapisu dokumentów zgód w formacie XACML.

3.	Możliwość przechowywania kolejnych wersji tego samego dokumentu. Możliwe jest automatyczne anulowanie poprzedniej wersji dokumentu w momencie utworzenia nowej wersji.
4.	Składowanie dokumentów elektronicznych z wykorzystaniem repozytorium EDM.
5.	Rejestrowanie wszystkich operacji wykonywanych przez użytkowników związanych z dokumentem zgodnych z profilem IHE ATNA.
6.	Przechowywanie w systemie i umożliwienie dostępu do wszystkich utworzonych dokumentów, w tym dokumentów archiwalnych oraz ukrytych – zgodnie z przydzielonymi uprawnieniami.
7.	Umożliwienie pobierania Dokumentów medycznych przechowywanych w repozytorium.
8.	Weryfikacja, przed pobraniem Dokumentu medycznego przez użytkownika, jego uprawnienia do tego dokumentu w module Kontrolera Polityki Dostępu.
9.	Obsługa rozróżniania następujących trybów wymiany Dokumentów medycznych: a. Kontynuacja leczenia b. Dla POZ c. Za zgodą pacjenta na dostęp do dokumentacji medycznej d. Tryb ratunkowy e. Dla autora Dokumentu medycznego f. Dla pacjenta, którego dotyczy dokument medyczny g. Dla podmiotu związanego umową podwykonania
10.	Umożliwienie zapisu Dokumentu medycznego w Regionalnym Repozytorium EDM a. z poziomu Lokalnego Repozytorium Dokumentów medycznych b. bezpośrednio przez HIS
11.	Umożliwienie przekazywania otrzymanego Dokumentu medycznego do walidacji przez moduł Walidatora Danych.
12.	Przeglądanie historii wszystkich operacji wykonanych na dokumentach przez użytkowników.
13.	Umożliwienie przechowywania danych tekstowych lub binarnych dowolnego formatu.
14.	Możliwość określenia rodzajów dokumentów przechowywanych w repozytorium EDM wraz z ich wersjonowaniem.
15.	Możliwość przechowywania dla każdego dokumentu dodatkowych informacji (metadanych) opis zawierający: 1) rodzaj i wersję, 2) rozmiar, 3) data utworzenia, 4) sumę kontrolną, 5) identyfikator osoby dodającej dokument, 6) identyfikator autora, 7) identyfikator komórki lub jednostki organizacyjnej, 8) identyfikator systemu zgłaszającego dokument.
16.	Przypisanie unikatowego identyfikatora dla każdego dokumentu w repozytorium EDM.
17.	Możliwość trwałego archiwizowania dokumentów bez opcji usunięcia lub modyfikacji.
18.	Przechowywanie dokumentów oraz metadanych w sposób gwarantujący ich integralność.
19.	Możliwość organizacji przechowywania dokumentów w różnych lokalizacjach dyskowych w zależności od: rodzaju, jednostki/komórki, systemu zgłaszającego, dowolnego warunku

	konfigurowalnego
20.	Dostęp do dokumentów i metadanych przez usługę sieciową (web service).
21.	Zabezpieczenie komunikacji z usługą dostępową przez SSL oraz profilem XDS.b.
22.	Możliwość wyszukiwania i pobierania przez usługę dostępową metadanych dokumentów przy pomocy wielokryterialnych zapytań.
23.	Wyszukiwanie dokumentów na podstawie metadanych, bez odczytu ich treści.
24.	Możliwość pobierania przez usługę dostępową ustawień dla rodzajów i wersji dokumentów.
25.	Możliwość pobierania przez usługę dostępową treści dokumentów.
26.	Przechowywanie logu wszystkich operacji na dokumentach z informacją o osobie wykonującej.

II.4.5.4 Kontroler Polityki Dostępu

1.	Obsługa sprawdzania uprawnienia dostępu użytkownika do danych przy użyciu metadanych Dokumentu medycznego oraz zadeklarowanego trybu dostępu.
2.	Obsługa rozróżnienia przynajmniej następujących trybów dostępu do danych: a) Kontynuacja leczenia b) Dla POZ c) Za zgodą pacjenta na dostęp do dokumentacji medycznej d) Tryb ratunkowy e) Dla autora Dokumentu medycznego f) Dla pacjenta, którego dotyczy dokument medyczny g) Dla podmiotu związanego umową podwykonania
3.	Umożliwienie weryfikacji uprawnień do danych poprzez weryfikację w rejestrze zgód Platformy P1 zgody pacjenta na dostęp do Dokumentu medycznego.

II.4.5.4.1 Walidator Danych

1.	Umożliwienie weryfikacji podpisu elektronicznego na Dokumencie medycznym.
2.	Obsługa weryfikacji wszystkich rodzajów podpisu elektronicznego przewidzianych prawem dla Dokumentów i Danych medycznych, w szczególności zgodnie z regulacjami prawnymi w zakresie sposobów podpisywania dokumentacji medycznej, wydanymi na podstawie art. 30 ust. 1 Ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (tj. Dz.U. z 2020 r. poz 849 z późń. zm.).
3.	Umożliwienie weryfikacji zgodności Dokumentu medycznego z HL7 CDA
3.	Umożliwienie weryfikacji zgodności Dokumentu medycznego z DICOM.
4.	Umożliwienie weryfikacji zgodności Dokumentu medycznego z XACML.

II.4.5.4.2 Regionalny Moduł Uwierzytelniania i Autoryzacji

1.	Umożliwienie pobierania tokenów z Platformy P1 koniecznych do komunikacji z nią.
2.	Umożliwienie przechowywania i używania certyfikatu nadanego systemowi lokalnemu przez Platformę P1, do komunikacji z Platformą P1 przy obsłudze żądań do tego systemu.
3.	Umożliwienie uwierzytelnienia i autoryzacji systemów lokalnych.
4.	Umożliwienie zarządzania bazą systemów lokalnych, ich uprawnieniami w Platformie i metodami uwierzytelnienia.
5.	Obsługa generowania tokenów SAML na potrzeby uwierzytelnienia użytkowników zapisujących, wyszukujących lub pobierających dokumenty medyczne z Regionalnego Repozytorium EDM.
6.	Umożliwienie tworzenia kontekstu dla żądań przychodzących z systemów zewnętrznych.
7.	Dostęp do danych musi być oparty na uprawnieniach użytkowników i być rozliczalny.
8.	Uprawnienia użytkowników są nadawane na zasadzie najmniejszego uprzywilejowania.
9.	Uprawnienia użytkowników są łączone w role systemowe.

II.4.5.4.3 Regionalne Repozytorium zdarzeń na potrzeby audytu

1.	Logowanie zdarzeń błędów działania aplikacji.
2.	Logowanie zdarzeń naruszeń zasad bezpieczeństwa.
3.	Logowanie zdarzeń komunikacji pomiędzy komponentami w zakresie określonym przez wykorzystywane profile IHE.
4.	Logi zdarzeń są zgodne z profilem IHE ATNA.
5.	Dla transakcji innych niż zgodne z profilami IHE określona jest struktura logu bazująca na strukturze przewidzianej w profilu IHE ATNA.
6.	Logowanie zdarzeń walidacji danych oraz wykrytych błędów walidacji danych.
7.	Logowanie zdarzeń modyfikacji zgody pacjenta.
8.	Logowanie zdarzeń udostępniania danych osobowych.
9.	Umożliwienie wyszukiwania komunikatów zdarzeń.
10.	Umożliwienie przekazywania komunikatów zdarzeń do rejestru zdarzeń Platformy P1.

11.	Umożliwienie generowania zgodnych z wymogami RODO raportów z logów zdarzeń związanych z przetwarzaniem danych osobowych.

II.4.5.4.4 Moduł administracyjny

1.	Umożliwienie pobierania i wyświetlania Dokumentów medycznych z Regionalnego Repozytorium EDM.
2.	Umożliwienie usuwania Dokumentu medycznego z Regionalnego Repozytorium EDM.
3.	Umożliwienie zarządzania bazą repozytoriów Dokumentów EDM.
4.	Umożliwienie zarządzania słownikami ról i uprawnień użytkowników systemów lokalnych.
5.	Umożliwienie zarządzania kontami użytkowników
6.	Obsługa graficznego interfejsu użytkownika.
7.	Zgodność graficznego interfejsu użytkownika z wymaganiami WCAG w wersji minimum 2.1 na poziomie minimum AA.

II.4.5.4.5 Baza danych dla Regionalnego repozytorium EDM

Lp.	**Bazy danych – Wymagania funkcjonalne**
1.	Relacyjna baza danych
2.	Funkcjonalności systemu bazy danych identyczne na 64-bitowe platformy Unix (Solaris dla procesorów SPARC/x86-64, IBM AIX), Intel Linux 64-bit, MS Windows 64bit.
3.	Możliwość migracji struktur bazy danych i danych pomiędzy ww. platformami bez konieczności rekompilacji aplikacji bądź migracji środowiska aplikacyjnego.
4.	Wsparcie dla wielu ustawień narodowych i wielu zestawów znaków (włącznie z Unicode).
5.	Brak formalnych ograniczeń na liczbę tabel i indeksów w bazie danych oraz na ich rozmiar (liczbę wierszy).
6.	Wsparcie dla procedur i funkcji składowanych w bazie danych.
7.	Wsparcie dla języków proceduralnych, blokowych (umożliwiającym deklarowanie zmiennych wewnątrz bloku), oraz wspierających obsługę wyjątków.
8.	Kompilację procedur składowanych w bazie danych do postaci kodu binarnego.
9.	Wymuszanie złożoności hasła Użytkownika, czasu życia hasła, sprawdzanie historii haseł, blokowanie konta przez administratora bądź w przypadku przekroczenia limitu nieudanych logowań.

10.	Określanie przywilejów użytkowników bazy danych za pomocą przywilejów systemowych (np. prawo do podłączenia się do bazy danych - czyli utworzenia sesji, prawo do tworzenia tabel itd.) oraz przywilejów dostępu do obiektów aplikacyjnych (np. odczytu / modyfikacji tabeli, wykonania procedury).
11.	Nadawanie przywilejów za pośrednictwem mechanizmu grup użytkowników / ról bazodanowych. W danej chwili użytkownik może mieć aktywny dowolny podzbiór nadanych ról bazodanowych.
12.	Wykonywanie i katalogowanie kopii bezpieczeństwa bezpośrednio przez serwer bazy danych. Zautomatyzowanego usuwania zbędnych kopii bezpieczeństwa przy zachowaniu odpowiedniej liczby kopii nadmiarowych - stosownie do założonej polityki nadmiarowości backup'ów.
13.	Wykonywanie kopii bezpieczeństwa w trybie offline oraz w trybie online.
14.	Zaimplementowanie polityki bezpieczeństwa regulującej dostęp do danych na poziomie pojedynczych wierszy w tabelach. Mechanizm ten powinien być realizowany za pomocą mechanizmów silnika bazy danych i powinien być przezroczysty dla aplikacji.
15.	Ochrona poufności i integralności informacji.
16.	Szyfrowanie informacji w bazie danych Warstwy regionalnej w obszarach wewnętrznym oraz sieciowym niezależny od aplikacji.
17.	Rejestrowanie zdarzeń silnika bazy danych w czasie rzeczywistym.
18.	Wykonywanie niektórych operacji związanych z utrzymaniem bazy danych bez konieczności pozbawienia dostępu użytkowników do danych. W szczególności dotyczy to tworzenia / przebudowywania indeksów oraz reorganizacji bądź redefinicji tabel.
19.	Zakładanie/przebudowywanie indeksów online bez konieczności odłączenia użytkowników operujących (zapytania, operacje insert, update, delete) na tabelach podlegających indeksowaniu.

II.4.5.5 Portal Projektu ZeZ

L.p.	Wymagania ogólne
1.	Architektury wdrażanych systemów muszą zapewniać pełną integrację wszystkich jego elementów oraz muszą być wykonane w taki sposób, by uniknąć redundancji danych. Redundancja danych w poszczególnych systemach jest dopuszczalna tylko na potrzeby tworzenia kopii zapasowych.
2.	Systemy muszą zapewniać przetwarzanie danych w ramach jednej lub wielu instancji bazy danych.
3.	Wymaga się od Wykonawcy stosowania w poszczególnych systemach jednolitych rozwiązań, w szczególności stosowania wzorców architektonicznych - komponenty tego samego typu muszą być implementowane w ten sam sposób (poprzez użycie tego samego wzorca).
4.	Systemy muszą działać w środowisku 64 bitowym.
5.	Systemy muszą posiadać budowę komponentową, opartą o Web Services, w której współdziałające komponenty komunikują się za pomocą szyfrowanych protokołów sieciowych

	(np. SSL/TLS, HTTPS), z wykorzystaniem otwartych standardów takich jak XML, JSON.
6.	Systemy muszą zapewniać zaszyfrowaną transmisję danych między użytkownikiem a serwerem.
7.	Systemy muszą współpracować z urządzeniami peryferyjnymi, w tym z drukarkami (lokalnymi, sieciowymi), skanerami (lokalnymi, sieciowymi), kserokopiarkami, faksami itp.
8.	Podstawą dla realizacji systemów muszą być wymagania zawarte 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 (KRI).
9.	Interoperacyjność Systemu (Komponentu) e-usług musi być zagwarantowana poprzez jego budowę w modelu usługowym (§ 8.1. KRI), zorientowanym na świadczenie e-usług (Service Oriented Architecture – SOA), w którym wszystkie funkcjonalności systemu teleinformatycznego dostępne są z poziomu przeglądarki internetowej, bez konieczności instalowania jakiegokolwiek oprogramowania po stronie użytkownika korzystającego z Systemu (Komponentu) e-usług.
10.	Interoperacyjność systemów musi być osiągana poprzez: 1) ich jednolitość, rozumianą jako stosowanie kompatybilnych norm, standardów i procedur przez różne jednostki realizujące zadania publiczne, posiadające dostęp do systemu, 2) ich zgodność, rozumianą jako przydatność produktów, procesów lub usług przeznaczonych do ich wspólnego użytkowania.
11.	Interoperacyjność systemów musi być osiągana na poziomach: 1) organizacyjnym, gwarantującym: a) dostęp do aktualnego systemu, b) przepływ informacji w systemie. 2) semantycznym, gwarantującym: a) stosowanie struktur danych i znaczenia danych w tych strukturach, zgodnych z KRI, b) wzajemną referencyjność i harmonizację danych systemu. 3) technologicznym, gwarantującym: a) neutralność technologiczną systemu.
12.	Systemy muszą zapewniać realizację zasady reuse, czyli rozwiązania z zakresu ponownego wykorzystania informacji na wielu poziomach, w tym na poziomie organizacyjnym, semantycznym i technologicznym.
13.	Wykonawca jest zobowiązany do dostarczenia rozwiązań oprogramowania zgodnie z przedstawioną lub własną koncepcją spełniającą wszystkie przedstawione wymagania. W szczególności Wykonawca może pogrupować funkcjonalności i wymagania w innym układzie obejmującym jeden lub więcej przedstawionych modułów.
	Wymagania dotyczące Portalu Projektu ZeZ
14.	Wykonawca musi wykonać i dostarczyć Zamawiającemu Portal Projektu ZeZ w ramach Zamówienia.
15.	Wykonawca musi przedstawić Zamawiającemu wykaz wszystkich licencji niezbędnych do wytworzenia i prawidłowego działania Portalu. W sytuacji, gdy Zamawiający nie zgodzi się na wykorzystywanie danego komercyjnego rozwiązania/danej licencji, z uwagi na jej koszt (związany z opłatami z tytułu utrzymania), Wykonawca w porozumieniu z Zamawiającym

	wybierze inne, dogodne dla Zamawiającego rozwiązanie open source bądź komercyjne.
16.	Portal musi być zgodny z aktualnie obowiązującymi przepisami i wytycznymi, w tym przede wszystkim: 1) ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tj. Dz.U. z 2017 r. poz. 570 z późn. zm.) wraz z aktami wykonawczymi, 2) ustawą z 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (tj. Dz.U. z 2017 r. poz. 1219 z późn. zm.) wraz z aktami wykonawczymi, 3) ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000, 1669), 4) rozporządzeniem 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. 2012 poz. 526 z późn. zm.); a także z obowiązującym u Uczestnika Projektu systemem zarządzania bezpieczeństwem informacji.
17.	Wykonawca musi zapewnić zgodność Portalu z przepisami UE dotyczącymi obowiązków informacyjnych w zakresie zaprojektowania i oznaczania stron internetowych oraz Wytycznymi ministra właściwego ds. rozwoju ww. zakresie, w szczególności Podręcznikiem wnioskodawcy i beneficjenta programów polityki spójności 2014-2020 w zakresie informacji i promocji z dnia 21 lipca 2017r.
18.	Zasady promocji i oznaczania stron projektu znajdują się pod następującym adresem: https://www.funduszeeuropejskie.gov.pl/strony/o-funduszach/promocja/zasady-promocji-i-oznakowania-projektow-1/zasady-promocji-i-oznakowania-projektow-wersja-aktualna-od-1-stycznia-2018-roku/
19.	Zamawiający dostarczy Wykonawcy elementy graficzne m.in. logotypy, które Wykonawca jest zobowiązany uwzględnić w projekcie graficznym Portalu.
20.	Wykonawca musi przedstawić Zamawiającemu do akceptacji projekt graficzny, layout, szablony wizualne Portalu, przed jej uruchomieniem.
21.	Portal musi umożliwiać dostęp do wszystkich e-usług poprzez przeglądarkę internetową.
22.	Graficzny interfejs użytkownika (GUI) Portalu musi być wytworzony w technologii wielowarstwowej, umożliwiającej pracę przez przeglądarkę internetową wspierającą języki przynajmniej: HTML5, XHTML, CSS3, JavaScript (m.in. Chrome, Firefox, Edge).
23.	GUI musi być skalowalny do różnych rozdzielczości ekranu (responsywny).
24.	Wykonawca musi zapewnić kodowanie Portalu zgodne ze standardami W3C.
25.	Do poprawnego działania Portalu, nie może być wymagana instalacja żadnego dodatkowego oprogramowania na stacji roboczej Użytkownika. Poprawne działanie i wyświetlanie interfejsu użytkownika musi odbywać się jedynie przez aktualne, na dzień składania ofert, stabilne wersje przeglądarek internetowych wymienionych w wymaganiu powyżej.
26.	Portal musi posiadać prosty i przejrzysty interfejs użytkownika.
27.	Językiem Interfejsu użytkownika Portalu oraz dokumentacji powstałej w ramach realizacji Zamówienia musi być język polski.
28.	Interfejs użytkownika Portalu e-Usług musi być zgodny ze standardami WCAG 2.1 (Web Content Accessibility Guidelines - https://www.w3.org/TR/WCAG21/) z uwzględnieniem poziomu AA, co zapewni, że udostępniane dzięki systemowi treści i usługi będą dostępne dla

	osób niepełnosprawnych.
29.	Portal musi przejść kompleksowe sprawdzenie wszystkich stron w oparciu o metodę oceny dostępności cyfrowej stron internetowych zgodnie z zasadami WCAG 2.1, gdzie wynikiem badania będzie raport, w którym wykazana zostanie zgodność strony ze standardem WCAG 2.1 na poziomie AA;
30.	Portal musi zawierać deklarację dostępności, dokument o dostępności strony, którego umieszczanie w Internecie wymaga ustawa o dostępności cyfrowej. Deklaracja musi być sporządzona wg wzoru Ministerstwa Cyfryzacji i widoczna na każdej stronie serwisu.
31.	Portal musi umożliwiać udostępnienie informacji (m.in. o e-usługach) bez konieczności posiadania konta użytkownika.
32.	Sposób dostępu do e-usług w ramach danego Portalu musi być spójny graficznie i funkcjonalnie.
33.	Portal musi zawierać przede wszystkim: 1) katalog dostępnych e-usług u Partnerów Projektu, 2) opis dostępnych e-usług, 3) sekcję informacyjną: a) aktualności (tzw. news room) – bieżące informacje z zakresu funkcjonowania systemu ochrony zdrowia w regionie z możliwością bezpośredniego dodawania aktualności przez podmioty lecznicze, po wstępnej weryfikacji treści przez administratora, b) badanie jakości poprzez ankiety i wnioski – aktywne formularze umożliwiające pacjentom przekazywanie uwag i wniosków odnoszących się do funkcjonowania podmiotów leczniczych, udzielanych przez nie świadczeń oraz prowadzenie regularnych badań ankietowych związanych z badaniami poziomu satysfakcji pacjentów, c) świadczenia zdrowotne podmiotów leczniczych (wydzielona przestrzeń dla każdego Partnera Projektu). Powinna zawierać Informacje bieżące z poszczególnych podmiotów leczniczych oraz informacje o zakresie funkcjonowania, oddziałach, poradniach, miejscach udzielania świadczeń oraz przekierowania do lokalnego modułu e-Rejestracji; d) użyteczne adresy www: możliwość wprowadzenia adresów do innyh podmiotów leczniczych w regionie nie będących Partnerem Projektu, aptek, dostęp do IKP, PUE ZUS i inne;, e) informacje o Projekcie „Zachodniopomorskie e-Zdrowie”: założenia, cele, korzyści dla pacjentów, kalendarium prac, serwis fotograficzny itp. 4) Sekcję pomocy.
34.	Portal musi umożliwiać utworzenie Strefy dla Partnera Projektu, dostępnej po uwierzytelnieniu przez podmiot, udostępniającej: 1) Platformę Zakupową SPZOZ (system dostarczany i wdrażany w ramach odrębnego postępowania) 2) Informacje, zestawienia analityczne publikowane przez organ tworzący (Urząd Marszałkowski) z zakresu świadczonych usług: wyniki, benchmarki itp., 3) Wyniki z badania jakości.

35.	Struktura Portalu musi być intuicyjna oraz przejrzysta dla użytkownika.
36.	Szczegółowa struktura musi być przedmiotem koncepcji sporządzonej przez Wykonawcę na etapie analizy przedwdrożeniowej, uzgodnionej z Zamawiającym i przez niego zatwierdzonej.
37.	Wykonawca zapewni system zarządzania treścią Portalu (CMS – Content Management System). System CMS musi posiadać wbudowane zabezpieczenia (m.in. ochrona przed próbą nieautoryzowanego dostępu do panelu sterowania, panel administracyjny dostępny poprzez połączenie szyfrowane), narzędzie do edycji treści w trybie WYSIWYG, usuwanie/podmiana/wersjonowanie dokumentów, podgląd Portalu przed publikacją treści.
38.	Wymaga się, aby Portal był skalowalny, umożliwiając obsługę zwiększającej się liczby użytkowników i dokumentów oraz udostępniając mechanizmy „load balancing", cache stron i „failover".
39.	Wykonawca musi zapewnić w ramach Portalu mechanizm, umożliwiający szybkie (automatyczne zgodnie z konfiguracją lub na żądanie Administratorów) uruchomienie wyświetlania informacji o czasowej niedostępności portalu z przyczyn technicznych.
40.	Wymaga się, aby po uruchomieniu Portalu Wykonawca sporządził dokumentację powykonawczą Portalu, a także przeprowadził szkolenie z obsługi CMS dla wybranych pracowników Zamawiającego wraz z dostarczeniem instrukcji stanowiskowej. Dokumentacja powykonawcza musi być aktualizowana przez Wykonawcę po każdej zmianie w oprogramowaniu.
41.	Utrzymywanie i prowadzenie Portalu musi być realizowane w infrastrukturze Zamawiającego. Uruchomienie Portalu wraz ze wszystkimi niezbędnymi elementami w infrastrukturze Zamawiającego przeprowadzi Wykonawca. Zamawiający dostarczy informacje o domenie i subdomenach dla każdego z Portali.
42.	Wykonawca w ramach otrzymanego wynagrodzenia musi przenieść na Zamawiającego prawa autorskie do Portalu (CMS, treść stron www wytworzonych za pomocą CMS) rozumianego jako utwór w rozumieniu ustawy o prawach autorskich i prawach pokrewnych, w tym przeniesienie praw autorskich do projektu graficznego, kodu źródłowego Portalu, elementów graficznych Portalu oraz oprogramowania CMS wraz z kodem źródłowym do tego oprogramowania.
43.	Kody źródłowe Portalu oraz oprogramowania CMS muszą być jawne i dostarczone w takiej postaci, aby Zamawiający był w stanie prześledzić funkcjonowanie Portalu m.in. pod kątem bezpieczeństwa.
44.	Wraz z Portalem, Wykonawca musi dostarczyć narzędzia do administrowania Portalem (konfiguracja, ustalanie praw dostępu, postępowanie w przypadku awarii, backup & restore). Narzędzia nie mogą wymagać specjalistycznej wiedzy od administratora, który będzie z nich korzystał.
45.	W zakresie nieopisanym w niniejszym rozdziale, Wykonawca zobowiązany jest uzyskać zgodę (akceptację) Zamawiającego na wszelkie dokonywane działania, czynności, prace, i przygotowywane przez Wykonawcę dokumenty oraz uwzględnić wszelkie uwagi i sugestie Zamawiającego w związku z realizacją Portalu.

II.4.6 Wymagania dotyczące integracji

L.p.	Opis wymagań
1.	Bezpieczeństwo: 1) system musi zapewniać przesyłanie danych z wykorzystaniem bezpiecznego kanału komunikacji - musi umożliwiać szyfrowanie transmisji danych co najmniej pomiędzy urządzeniami/systemami klienta: komputerami, urządzeniami mobilnymi itp. a pierwszym komponentem systemu, na którym są one przetwarzane, 2) System musi zapewniać dedykowane mechanizmy obsługi uprawnień, pozwalające na tworzenie i przydzielanie uprawnień użytkownikom osobowym (w ramach Panelu administracyjnego) jak i innym systemom informatycznym. 3) funkcjonalności związane z udostępnianiem danych muszą być dostępne tylko dla uwierzytelnionych użytkowników.
2.	Architektura rozwiązania: 1) system musi posiadać modułową budowę - preferowana architektura oparta o mikrousługi, podsystemy funkcjonalne, 2) należy zapewnić możliwość skalowania horyzontalnego wybranych modułów systemu (w zależności od obciążenia), 3) system musi udostępniać interfejs programowy (API) umożliwiający jego integrację z innym oprogramowaniem działającym obecnie lub w przyszłości u Zamawiającego, 4) architektura systemu musi pozwalać na wdrożenie go w wariancie wysokiej dostępności (ang. high availability) poprzez równoczesne działanie jego "zapasowej" instancji.
3.	Oprogramowanie Serwera WWW hostującego system eUsług musi być programem międzyplatformowym i musi być dostępne co najmniej w systemach operacyjnych Linux i Windows.
4.	Stosowane technologie: 1) wykorzystywane technologie muszą być zgodne z wytycznymi konsorcjum W3C wyznaczającym standardy dokumentów www, 2) stosowanie najnowszych wersji odmiany języka HTML wersja HTML5, 3) stosowane technologie są akceptowane i wspierane przez producentów popularnych przeglądarek www, 4) stosowanie popularnych i ogólnie dostępnych bibliotek i frameworków takich jak: Jquery, Angular, Jquery UI, Bootstrap i tym podobne.
5.	Modele wdrożenia: 1) zakłada się dostarczenie gotowych do uruchomienia komponentów systemu wraz ze wszystkimi zależnościami i domyślną konfiguracją - preferowane wykorzystanie technologii konteneryzacji, 2) system podczas eksploatacji musi zapisywać logi z działania w postaci umożliwiającej ich dalsze przetwarzanie w dedykowanych ku temu narzędziach (np. Logstash).
6.	Rozwiązanie musi korzystać z wybranych profili IHE opisanych w Modelu realizacyjnym w rozdziale III.
7.	Przygotowane przez Wykonawcę interfejsy API muszą posiadać dokumentację integracyjną

	opisującą rozwiązanie w stopniu wystarczającym do umożliwienia integracji dowolnej liczby Partnerów, w tym w szczególności systemów dziedzinowych (systemów źródłowych HIS) Partnerów Projektu.

II.4.6.1 Przygotowanie dokumentacji integracyjnej oprogramowania warstwy lokalnej z warstwą regionalną - Regionalne Repozytorium EDM <-> Lokalne systemy HIS

Dokumentacja integracyjna oprogramowania warstwy lokalnej z warstwą regionalną.

Wymagana minimalna zawartość dokumentacji:

1. Architektura systemu
   - 1.1. Założenia w zakresie udostępniania i wymiany EDM – koncepcja
     - zakres i format wymienianej dokumentacji medycznej,
     - zakres metadanych wykorzystywanych do wyszukiwania wymienianych dokumentów,
     - zasady bezpieczeństwa i poufności wymiany dokumentów medycznych,
     - standardy komunikacji,
     - niezbędne wymagania infrastrukturalne.
   - 1.2. Opis architektury logicznej odzwierciedlającej poszczególne zasoby pomiędzy strukturami integrowanych obszarów
   - 1.3. Punkty dostępowe do każdego z podsystemu przypisanej struktury
   - 1.4. Opisanie możliwych wyników odpowiedzi wraz z ich znaczeniem i możliwym scenariuszem
   - 1.5. Opis mechanizmów dot. interwalów czasowych zasilania w dane wraz ze scenariuszami zapasowymi
   - 1.6. Opis możliwych interfejsów wraz z określeniem możliwych scenariuszy użycia
   - 1.7. Wskazanie modeli transakcji i opisanie poszczególnych typów
   - 1.8. Obiekty używane w transakcjach i ich znaczenie
   - 1.9. Struktura domen XDS w projekcie
2. Warstwy i komponenty warstwy regionalnej
   - 2.1. Regionalne repozytorium dokumentów medycznych
   - 2.2. Walidator dokumentów
   - 2.3. Komponent administracyjny
   - 2.4. Regionalne repozytorium zdarzeń na potrzeby audytu
3. Zasady przynależności podmiotów leczniczych do repozytorium regionalnego
   - 3.1. Procedura nadawania uprawnień dostępu do repozytorium
   - 3.2. Przebieg procedury nadawania uprawnień dostępu
4. Podstawowe operacje
   - 4.1. Rejestracja repozytorium podmiotu leczniczego
   - 4.2. Rejestracja danych dostępowych repozytorium podmiotu leczniczego
   - 4.3. Przekazywanie dokumentów medycznych do repozytorium i ich rejestracja w P1
   - 4.4. Wyszukiwanie dokumentów w rejestrze dokumentów P1 i ich pobieranie z repozytorium regionalnego
5. Zasady operacyjne

5.1. Zasady aktualizacji i udostępniania nowej wersji systemu
5.2. Zasady przechowywania i retencji danych oraz logów
5.3. Zasady postępowania w przypadku niedostępności systemu
5.4. Odtwarzanie po awarii
6. Diagramy przepływu danych oraz transakcji/komunikacji

Wykonawca zobowiązany jest do przygotowania a następnie udostępnienia ww. Dokumentacji integracyjnej w ciągu 3 miesięcy od podpisania umowy.

W ramach umowy przez cały okres gwarancji Wykonawca będzie świadczył usługę wsparcia w zakresie przygotowanego interfejsu API i dokumentacji integracyjnej w zakresie:

1) udzielanie konsultacji, porad, wsparcia technicznego w dni robocze w godzinach od 7.00 do 15.00 w języku polskim, przy czym: konsultacje i porady będą udzielane na bieżąco podczas rozmowy telefonicznej lub w postaci elektronicznej, jednak nie później niż w ciągu 3 dni roboczych od skierowania zapytania,
2) Wsparcie techniczne w zakresie integracji z wykorzystaniem interfejsu API dla wykonawców podłączających systemy szpitalne do wytworzonych e-usług w Warstwie Regionalnej wraz z przeprowadzaniem obustronnych testów,
3) Implementacja poprawek (na bazie zgłoszonych błędów) w interfejsie API i aktualizacji dokumentacji integracyjnej.

II.4.7 Instruktaże stanowiskowe

1. Z uwagi na to, iż w ramach projektu planuje się wdrożenie specjalistycznego oprogramowania i aplikacji, konieczne jest przeszkolenie personelu Zamawiającego oraz personelu Partnerów korzystających z wdrożonych e-usług. W związku z tym w ramach tego zadania zostaną przeprowadzone instruktaże stanowiskowe.
2. Wykonawca przeprowadzi instruktaże stanowiskowe w siedzibie Zamawiającego lub z wykorzystaniem platformy e-learningowej lub zdalnie. Zamawiający udostępni pomieszczenie celem przeprowadzenia instruktaży stanowiskowych.
3. Zamawiający dopuszcza, aby Szkolenia były realizowane w trybie tradycyjnego szkolenia w grupach po max. 10 osób w klasie lub w technologii e-Learning lub zdalnie dla danego obszaru merytorycznego. Zamawiający wskaże formę instruktaży dla danych obszarów merytorycznych.
4. Szkolenia zdalne będą prowadzone za pomocą dedykowanej platformy internetowej dostarczonej przez Wykonawcę.
5. Wykonawca zainstaluje na serwerze Zamawiającego platformę e-learning. Dopuszcza się udostępnienie platformy bez instalacji na serwerach Zamawiającego.
6. Na etapie przygotowania wdrożenia Wykonawca przygotuje dane do logowania do systemu szkoleń.
7. Platforma szkoleniowa będzie dostępna przez do 12 miesięcy od zakończenia wdrożenia.

8. W przypadku szkolenia e-learningowego wymaga się aby każdy etap składał się z:

1.	Części lekcyjnej (animacji trwającej ok. 6-8 minut) podzielonej na kroki.
2.	- w trakcie trwania animacji po kilku krokach będzie występowało ćwiczenie (około 2 ćwiczeń, gdzie ćwiczenie będzie miało około 5 poleceń).
3.	Lekcja powinna zatrzymywać się, wyróżniać i wyraźnie podkreślać ważne elementy.
4.	W czasie trwania lekcji musi być możliwość cofania i zatrzymania lekcji.
5.	Po zdanym egzaminie użytkownik będzie miał możliwość dowolnego poruszania się po lekcji do czasu wygaśnięcia uprawnień na platformie.
6.	Lekcje ogólne nt. interfejsu i standardów aplikacji będą dołączane do różnych pakietów.
7.	Ćwiczenia powinny mieć charakter dobrze zdefiniowanego zadania. Jeśli użytkownik wykona nieprawidłowy ruch, program podpowie prawidłowy. Użytkownik dostanie kompletne opisane zadanie do wykonania.
8.	Tekst wypowiadany przez lektora musi być również wyświetlony na ekranie na żądanie użytkownika.
9.	Lekcje, ćwiczenia, będą pokazywać, w którym momencie przerabianego materiału jest użytkownik i ile kroków zostało do końca (liczbowo np. krok 7 z 30).

9. Na podstawie przekazanego przez Zamawiającego wykazu osób oraz przewidywanego terminu i czasu instruktażu stanowiskowego, Wykonawca zaproponuje harmonogram jak i podział na grupy.
10. Szczegółowy harmonogram realizacji instruktaży zostanie uzgodniony na etapie Analizy Przedwdrożeniowej.
11. Harmonogramy instruktaży muszą umożliwiać Zamawiającemu obecność na zajęciach z danego tematu przeznaczonych dla innych grup (Partnerów), z zastrzeżeniem, że na jednych zajęciach z danego tematu może być obecny co najmniej 1 pracownik Zamawiajacego.
12. Wykonawca nie ponosi odpowiedzialności za brak uczestnictwa użytkowników w zaplanowanych i ujętych w harmonogramie instruktażach stanowiskowych.
13. Instruktaże stanowiskowe użytkowników oprogramowania RSI i administratora będą musiały spełniać następujące wymagania:
    1) zajęcia muszą odbywać się w godzinach od godz. 8.00 do 15.00,
    2) zajęcia nie będą mogły trwać dłużej niż 6 godzin dziennie,
14. Za skuteczne przeprowadzenie instruktażu stanowiskowego uważa się dostępność w ustalonym miejscu i terminie przedstawicieli Wykonawcy, gotowych przeprowadzić instruktaż zgodnie z ustalonym harmonogramem.
15. Wykonawca w ramach instruktażu stanowiskowego przekaże instrukcje do wdrożonego Systemu oraz materiały szkoleniowe. Instruktaże stanowiskowe będą prowadzone w języku polskim.
16. W ramach przeprowadzonych instruktaży stanowiskowych wymaga się:

1) przekazania wiedzy niezbędnej do poprawnego użytkowania wdrożonego systemu, jego zakresu funkcjonalnego,

2) przekazania wiedza w zakresie tworzenia i gromadzenia informacji, tworzeniem i gromadzeniem dokumentów, wykonywaniem analiz, sprawozdań i raportów.

17. Zakres instruktaży stanowiskowych musi objąć teorię i praktykę (musi być zapewniona odpowiednia liczba ćwiczeń – minimum w stosunku 50% / 50%) tak, aby użytkownicy mogli podjąć samodzielnie działania użytkowania wdrożonego oprogramowania RSI.

18. Instruktaże stanowiskowe muszą być prowadzone w dwóch kategoriach:

3) dla użytkowników oprogramowania RSI – min. 4 dni po 6h (w sumie 24h),

4) dla administratorów – min. 3 dni po 8h (w sumie 24h) .

19. Szacowana liczba użytkowników planowanych do instruktaży stanowiskowych:

1) Pracownicy Zamawiającego - 8osób,
2) Pracownicy Partnerów Projektu - 26osób,
3) Administratorzy - 8osoby.

20. Po ukończeniu instruktaży stanowiskowych uczestnicy muszą w szczególności posiadać następujące umiejętności:

1) posługiwać się w pełni samodzielnie wdrożonym oprogramowaniem RSI i jego modułami odpowiednio do swojej roli,

2) znać i rozumieć ich funkcjonowanie w Systemie.

21. Administratorzy po zakończeniu instruktaży muszą w szczególności posiadać następujące umiejętności:

1) wykonywać czynności administracyjne a także instalacji oprogramowania systemowego i narzędziowego oraz oprogramowania RSI,

2) znać i realizować procedury backupu,

3) znać wytyczne w zakresie polityki bezpieczeństwa i umieć je stosować.

4) znać typowe zagrożenia i problemy związane z funkcjonowaniem Systemu, a także sposoby ich wykrywania oraz przeciwdziałania,

5) umieć instalować, konfigurować, rekonfigurować, monitorować i prawidłowo eksploatować dostarczony Sprzęt i Oprogramowanie, jak również znać jego wdrożoną konfigurację.

Rozdział III. Gwarancja

III.1.1 Okres gwarancji

1. Wykonawca w ramach realizacji Przedmiotu Zamówienia udzieli Zamawiającemu gwarancji jakości (dalej zwanej „gwarancją") na niniejszy przedmiot zamówienia:

a. Modernizacja sieci teleinformatycznej:

Poz. OPZ	Opis**	Okres gwarancji (minimalny)*
Rozdział II.1	**Modernizacja sieci teleinformatycznej**	
II.1.1	UTM	60 miesięcy
II.1.2	Przełącznik serwerowy LAN	60 miesięcy
II.1.3	Przełącznik zasobowy SAN	60 miesięcy
II.1.4	Szafa 42U z wyposażeniem	60 miesięcy
II.1.5	Konsola KVM-KMM	60 miesięcy

b. Infrastruktura serwerowa:

POZ. SOPZ	Opis**	Okres gwarancji (minimalny)*
ROZDZIAŁ II.2	**INFRASTRUKTURA SERWEROWA**	
II.2.1	Serwer lokalizacja nr 1	60 miesięcy
II.2.2	Serwer lokalizacja nr 2	60 miesięcy
II.2.3	Macierz dyskowa	60 miesięcy
II.2.4	Biblioteka taśmowa	60 miesięcy
II.2.5	Serwer kopii bezpieczeństwa	60 miesięcy
II.2.6	Deduplikator	60 miesięcy

c. Oprogramowanie systemowe i narzędziowe:

POZ. OPZ	Opis**	Okres gwarancji (minimalny)*
ROZDZIAŁ II.3	**OPROGRAMOWANIE SYSTEMOWE I NARZĘDZIOWE**	
II.3.1	Serwerowy system operacyjny	----------
II.3.2	Oprogramowanie wirtualizacyjne	60 miesięcy
II.3.3	Oprogramowanie backupowe	60 miesięcy
II.3.4	System ochrony aplikacji webowych oraz XML	60 miesięcy

d. dostawa i wdrożenie Regionalnego Systemu Informatycznego

Poz. OPZ	Opis	Okres gwarancji i nadzoru autorskiego (minimalny)
II.4	Dostawa i wdrożenie Regionalnego Systemu Informatycznego	60 miesięcy

* W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).

** W przypadku awarii nośników pozostają one własnością Zamawiającego.

2. Bieg terminów gwarancji określonych w ust. 1 będą rozpoczynać się z dniem podpisania Protokołu Odbioru Końcowego bez uwag przez Zamawiającego.
3. Naprawy gwarancyjne muszą być realizowane przez serwis producenta lub Autoryzowanego Partnera Serwisowego Producenta.
4. Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu.

III.1.2 Zakres gwarancji i nadzoru autorskiego dostarczonego oprogramowania aplikacyjnego

Nazwa	Opis
Serwis RSI	1. W okresie gwarancji Wykonawca będzie zobowiązany do nieodpłatnego usuwania Wad Przedmiotu Zamówienia rozumianych jako Błąd, Awaria lub lub Usterka zgodnie z definicjami, jak poniżej: 1) Wada - Każda nieprawidłowość w działaniu części lub całości RSI lub systemu informatycznego rozumiana jako niezgodność z SOPZ, Analizą Przedwdrożeniową i Dokumentacją (w tym określoną przez Wykonawcę dokumentacją systemu). Wady dzielą się na Błędy Awarie, Usterki. 2) **Błąd** – Wada powtarzalna, pojawiająca się za każdym razem w tym samym miejscu w Aplikacji na różnych stacjach roboczych (terminalach) i prowadzące w każdym przypadku do otrzymywania nieprawidłowych wyników, spowodowana uszkodzeniem lub utratą: kodu programu, struktur danych, zawartości bazy danych, integralności danych. 3) **Awaria –** Błąd krytyczny oznaczający sytuację, w której RSI lub jego Aplikacja lub element infrastruktury informatycznej w ogóle nie funkcjonuje lub nie jest realizowana jej kluczowa funkcjonalność bez działania której eksploatacja Aplikacji/urządzenia przestaje być zasadna. 4) **Usterka** - Błąd, mimo identyfikacji którego Aplikacja/urządzenie nadal funkcjonuje lecz jej/jego eksploatacja jest uciążliwa, skomplikowana lub spowolniona. 2. Przyjęcie zgłoszenia Wady przez Wykonawcę, odbywać się będzie poprzez dostępny on-line System Zgłaszania i przyjmowania uwag oraz Wad (dalej zwany

	SZ) przy czym: 1) System Zgłoszeń dostarczy Wykonawca (będzie on utrzymywany i administrowany przez Wykonawcę), wpis zgłoszenia do SZ będzie dokonywał Zamawiający, 2) za skuteczne przyjęcie zgłoszenia Wady uważa się będzie wprowadzenie przez Zamawiającego wpisu do SZ zawierającego opis zgłaszanej Wady i termin jej zgłoszenia; w razie trudności z dostępem on-line do SZ, zgłoszenia Wady mogą odbywać się także telefonicznie pod ustalonym numerem telefonu lub pisemnie na formularzu przesyłanym na ustalony adres e-mail, opcjonalnie faksem, których numery i adresy zostaną podane przez Wykonawcę w terminie 15 dni roboczych od dnia podpisania Umowy wraz ze wzorem formularza zgłoszenia Wady. 3. W przypadku, w którym wykonanie Umowy związane będzie z modernizacją lub rozbudową istniejącego oprogramowania (niniejszy OPZ zawiera dla aplikacji specyfikację funkcjonalną) , gwarancja obejmuje całość oprogramowania modernizowanego lub rozbudowywanego.
Konserwacja	1. Realizacja zadania zapewni Zamawiającemu poprawę jakości oraz poszerzenie zakresu funkcjonalnego oprogramowania aplikacyjnego, jak również dostosowanie tego oprogramowania do zmian czynników wewnętrznych organizacji Zamawiającego oraz zewnętrznych, będących efektem nowelizacji uwarunkowań prawnych. 2. W ramach Konserwacji Wykonawca zagwarantuje: 1) prowadzenie rejestru zgłaszanych przez użytkowników błędów ww. oprogramowania aplikacyjnego 2) wprowadzanie do ww. oprogramowania aplikacyjnego nowych funkcji oraz usprawnień już istniejących, stanowiących wynik inwencji twórczej producenta, 3) wprowadzanie do ww. oprogramowania aplikacyjnego zmian stanowiących konsekwencję wejścia w życie nowych aktów prawnych lub aktów prawnych zmieniających obowiązujący stan prawny, opublikowanych w postaci ustaw, rozporządzeń, itp. 4) wprowadzanie do oprogramowania aplikacyjnego zmian wymaganych przez wyszczególnione poniżej organizacje, w stosunku do których Zamawiający ma obowiązek prowadzenia sprawozdawczości, w szczególności: a) Ministerstwa Zdrowia, b) NFZ, c) Centrów Zdrowia Publicznego. 5) wprowadzanie w trybie pilnym do ww. oprogramowania aplikacyjnego zmian i poprawek usuwających stwierdzone błędy i luki we wbudowanych mechanizmach i funkcjach zabezpieczeń, 6) gotowość do odpłatnego wykonania na zlecenie Zamawiającego zaproponowanych przez niego modyfikacji ww. oprogramowania aplikacyjnego.
Konsultacje	Gotowość do świadczenia Zamawiającemu usługi pomocy technicznej i eksploatacyjnej w odniesieniu do ww. oprogramowania aplikacyjnego.

Tabela 1. Gwarancja dla Regionalnego Systemu Informatycznego – reżim realizacji serwisu

KWALIFIKACJA ZGŁOSZENIA WADY	OKRES DOSTĘPNOŚCI WYKONAWCY	ROZWIĄZANIE ZASTĘPCZE	CZAS REAKCJI WYKONAWCY	CZAS NAPRAWY
AWARIA	24/7/365	W CZASIE NAPRAWY, dopuszczalne rozwiązanie umożliwiające przekwalifikowanie na Błąd	niezwłocznie, nie później niż 4 godzin od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia
BŁĄD	W dni robocze pomiędzy 7 a 15 Zgłoszenie przesłane po 15 traktowane jest jak zgłoszenie przyjęte w następnym dniu roboczym o 7	W CZASIE NAPRAWY, dopuszczalne rozwiązanie umożliwiające przekwalifikowanie na Usterkę	niezwłocznie nie później niż 24 godziny robocze od dnia przyjęcia zgłoszenia	niezwłocznie nie później niż 10 dni roboczych od dnia przyjęcia zgłoszenia
USTERKA	W dni robocze pomiędzy 7 a 15 Zgłoszenie przesłane po 15 traktowane jest jak zgłoszenie przyjęte w następnym dniu roboczym o 7	nie dotyczy	niezwłocznie nie później niż 5 dni roboczych od dnia przyjęcia zgłoszenia	niezwłocznie nie później niż 30 dni roboczych od dnia przyjęcia zgłoszenia

III.1.3 Zakres asysty technicznej dla Oprogramowania

1. Warunkiem rozpoczęcia asysty technicznej jest podpisanie przez strony Protokołu Odbioru Końcowego bez uwag.
2. W ramach realizacji asysty technicznej Wykonawca zobowiązuje się na świadczenie 250 roboczogodzin asysty technicznej polegającej na:
   1) zapewnieniu Zamawiającemu pomocy w rozwiązaniu problemów i incydentów wynikłych w trakcie obsługi Oprogramowania tj:
      a. Analiza problemów zgłaszanych przez użytkowników Oprogramowania.
      b. Asysta przy określaniu i usuwaniu przyczyn oraz skutków zgłaszanych incydentów.
      c. Dostarczanie, instalacja (po uzyskaniu zgody Zamawiającego) i konfiguracja uaktualnień i nowych wersji dla Oprogramowania lub jego komponentów w przypadku zmian i aktualizacji oraz związanych z tym aktualizacji dostarczonej dokumentacji i przekazanych kodów źródłowych.
      d. Przeprowadzanie analiz oraz udzielanie konsultacji Zamawiającemu.
      e. Dokonywanie zmian konfiguracji Oprogramowania.
      f. Dokonywanie modyfikacji Oprogramowania.
      g. Opracowywanie i dostarczanie dokumentacji, w tym aktualizacji dokumentacji oraz dostarczanie dokumentacji wprowadzanych zmian.

   2) Zapewnienia usług rozwojowych rozumianych jako pula godzin rozwojowych do dyspozycji Zamawiającego na modyfikacje, ktorych nie dało się przewidzieć na etapie przygotowywania SWZ. Zamawiający przez jedną godzinę rozwojową rozumie czas w ilości 1h (60 min) jakie Wykonawca przeznacza na wdrożenie zgłoszonej przez Zamawiającego modyfikacji realizując m.in. takie usługi jak: analiza wymagań, prace programistyczne, wdrożenie.

      W ramach świadczenia usług rozwoju oprogramowania, Wykonawca zobowiązany jest do rozszerzenia funcjonalności Oprogramowania aplikacyjnego lub dziedzinowego wynikającego ze zlecenia przedstawionego przez Zamawiającego i zaakceptowanego przez Wykonawcę. Wszystkie wytworzone w ramach realizacji usług rozwoju Produkty będą podlegały procedurom odbiorowym. Odbiór Zamówienia usługi rozwoju zostanie potwierdzony przez Strony protokołem Odbioru Usługi Rozwojowej. Funkcjonalności wytworzone w ramach usług rozwoju podlegają gwarancji.

3. Dokonywanie okresowych (nie rzadziej niż co 6 m-cy) przeglądów gwarancyjnych dostarczonego Oprogramowania. W ramach przeprowadzanych okresowych przeglądów gwarancyjnych muszą być wykonane co najmniej następujące czynności:
   1) Weryfikacja poprawności działania oraz optymalizacja konfiguracji wszystkich komponentów wchodzących w skład Oprogramowania (systemy operacyjne, bazy danych, oprogramowanie narzędziowe, oprogramowanie dziedzinowe, oprogramowanie standardowe oprogramowanie Systemów itp).
   2) Analiza logów wszystkich komponentów Oprogramowania i podjęcie działań naprawczych w razie potrzeby.
   3) Aktualizacja (w razie potrzeby i po uzyskaniu uprzedniej zgody Zamawiającego) wersji poszczególnych komponentów wchodzących w skład Oprogramowania.

4. Proces realizacji asysty technicznej będzie przebiegał następująco:
   a. Zamawiający przekaże Wykonawcy drogą mailową zlecenie wykonania asysty technicznej. Zgłoszenie zawierać będzie co najmniej:
      a. Zakres prac do wykonania lub opis problemu do rozwiązania.
      b. Określenie proponowanego terminu realizacji (opcjonalnie).
      c. Określenie miejsca wykonania usługi (opcjonalnie).
5. W terminie nie dłuższym niż 3 dni robocze od dnia otrzymania zgłoszenia o asystę techniczną Wykonawca skontaktuje się z Zamawiającym w celu ustalenia szczegółowego zakresu prac, terminu realizacji i szacowanego wymiaru godzin realizacji asysty technicznej.
6. Po kontakcie z Zamawiającym, w terminie nie dłuższym niż 1 dzień roboczy (o ile Strony nie ustalą późniejszego terminu) Wykonawca rozpocznie realizację usługi.
7. Po wykonaniu każdorazowych prac związanych z asystą techniczną i uzyskaniem przez Wykonawcę potwierdzenia ich wykonania od Zamawiającego, Wykonawca przedstawi dokument – Raport z asysty technicznej, zawierający co najmniej:
   a. Opis wykonanych prac.
   b. Liczbę godzin poświęconą na wykonanie prac.
   c. Całkowitą liczbę godzin asysty technicznej zrealizowanych od początku trwania usługi, których realizacji została potwierdzona przez Zamawiającego.

2. Wykonawca ma prawo odmówić wykonania asysty technicznej o ile:
   a. Zamawiający wyczerpał przysługujący limit roboczogodzin lub zakończył się okres realizacji asysty technicznej.
   b. Realizacja asysty technicznej w zaproponowanym zakresie spowodowałaby przekroczenie przysługującego Zamawiającego limitu roboczogodzin asysty technicznej.
3. Zamawiający umożliwi Wykonawcy realizację usługi asysty technicznej poprzez udostępnienie wymaganych zasobów technicznych oraz niezbędnych pracowników Zamawiającego.

Zamawiający zastrzega sobie prawo do weryfikacji z udziałem ekspertów zewnętrznych ilości roboczogodzin na realizację usług wsparcia wnioskowanych przez Wykonawcę.

III.1.4 Reżimy realizacji serwisu w Infrastrukturze Sprzętowej

W okresie gwarancji Wykonawca będzie zobowiązany do nieodpłatnego usuwania Wad Przedmiotu Zamówienia (dotyczy infrastruktury sieci teleinformatycznej, infrastruktury serwerowej oraz sieciowej) rozumianych jako Awaria lub Usterka zgodnie z definicjami, jak poniżej:

1) **Awaria -** Kategoria Wady w Infrastrukturze Sprzętowej powodująca brak działania lub niepoprawne działanie Przedmiotu Zamówienia u Zamawiającego, uniemożliwiające jego użytkowanie. Sytuacja, w której Oprogramowanie w ogóle nie funkcjonuje lub nie jest możliwe realizowanie istotnych funkcjonalności Komponentów/Produktów Przedmiotu Zamówienia.

2) **Usterka -** Należy przez to rozumieć kategorię Wady w Infrastrukturze Sprzętowej oznaczającą funkcjonowanie niezgodne z opisem Dokumentacji oraz SOPZ, nie wpływającą istotnie na funkcjonowanie dostarczanego rozwiązania u Zamawiającego, utrudniającą pracę Użytkownikowi Zamawiającego.
3)

Tabela 2. Gwarancja dla modernizacji sieci teleinformatycznej:

1) UTM
2) Przełączniki
3) Konsola KVM
4) Szafa rack

KWALIFIKACJA ZGŁOSZENIA WADY	OKRES DOSTĘPNOŚCI WYKONAWCY (MOŻLIWOŚĆ ZGŁASZANIA WADY)	ROZWIĄZANIE ZASTĘPCZE	CZAS REAKCJI WYKONAWCY	CZAS NAPRAWY
AWARIA	24/7/365	niezwłocznie nie później niż 24 godziny od przyjęcia zgłoszenia	niezwłocznie, nie później niż 4 godziny od czasu przyjęcia zgłoszenia	niezwłocznie nie później niż 4 dni roboczych od dnia przyjęcia zgłoszenia
USTERKA	24/7/365	niezwłocznie nie później niż 3 dni roboczych od dnia przyjęcia zgłoszenia	niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia	niezwłocznie nie później niż 10 dni roboczych od dnia przyjęcia zgłoszenia

Tabela 3. Gwarancja dla Infrastruktury serwerowej:

1) Serwer lokalizacja nr 1,
2) Serwer lokalizacja nr 2,
3) Macierz dyskowa,
4) Biblioteka taśmowa.
5) Deduplikator

KWALIFIKACJA ZGŁOSZENIA WADY	OKRES DOSTĘPNOŚCI WYKONAWCY	ROZWIĄZANIE ZASTĘPCZE	CZAS REAKCJI WYKONAWCY	CZAS NAPRAWY
AWARIA	24/7/365	niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 4 godziny od czasu przyjęcia zgłoszenia	niezwłocznie nie później niż 4 dni roboczych od dnia przyjęcia zgłoszenia

USTERKA	24/7/365	niezwłocznie, nie później niż 3 dni od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 10 dni od czasu przyjęcia zgłoszenia

1. Dopuszcza się zmianę kwalifikacji zgłoszenia Wady, po uprzedniej zgodzie Zamawiającego. Do czasu potwierdzenia zmiany kwalifikacji, uznaje się za obowiązującą kwalifikację pierwotną.
2. Czasy naprawy mogą być inne niż wskazane w powyższych tabelach, jeżeli Zamawiający zaakceptuje zmianę kwalifikacji zgłoszenia, o której mowa w punkcie 2).
3. W przypadku braku możliwości usunięcia Wady lub przedstawienia rozwiązania zastępczego zdalnie, Wykonawca zobowiązany jest do świadczenia gwarancji bezpośrednio w lokalizacji Zamawiającego.
4. Usunięcie Wady Oprogramowania, nastąpi poprzez przekazanie poprawki lub nowej wersji. Każda nowa poprawka lub nowa wersja musi posiadać unikalny numer.
5. Wykonawca w okresie trwania gwarancji, do 5 dnia każdego miesiąca, przedstawi Zamawiającemu raport zawierający co najmniej: numer zgłoszenia, kwalifikację zgłoszenia, godzinę i datę zgłoszenia, temat zgłoszenia, status zgłoszenia, godzinę i datę usunięcia Wady, czas naprawy, wykonywania Serwisu - Oprogramowania na poniższych zasadach:
   1) wykonywania modyfikacji bez wezwania lub na pisemne zgłoszenie Zamawiającego w celu dostosowania wszystkich elementów Oprogramowania do obowiązujących przepisów prawnych,
   2) przekazania Zamawiającemu informacji o nowych wersjach Oprogramowania drogą elektroniczną na wskazany adres e-mail Zamawiającego,
   3) udostępniania nowych wersji Oprogramowania poprzez ustaloną witrynę internetową lub serwer ftp, w szczególności związanych z wejściem w życie nowych przepisów prawa lub zawierających nowe funkcjonalności; w przypadku, w którym udostępnianie następować będzie w związku ze zmianą przepisów prawa, Wykonawca zobowiązany będzie do jej dokonania na nie mniej niż 14 dni przed dniem wejścia w życie tych przepisów. W uzasadnionych przypadkach, Zamawiający dopuści, aby Wykonawca udostępnił odpowiednie zmiany w terminach umożliwiających Zamawiającemu wywiązanie się ze zmienionych przepisów prawa,
   4) każda nowa wersja musi posiadać unikalny numer,
   5) wraz z nową wersją Wykonawca zobowiązany jest do przekazania nowej wersji Dokumentacji Powykonawczej wraz z procedurą instalacji oraz informacją o parametryzacji i konfiguracji,
   6) udzielanie konsultacji, porad, wsparcia technicznego w zakresie wdrożenia oraz użytkowania Oprogramowania w dni robocze w godzinach od 7.00 do 15.00 w języku polskim, przy czym:

a) tryb zgłaszania: telefonicznie, e-mail, faxem lub poprzez System Zgłoszeń,

b) konsultacje i porady będą udzielane na bieżąco podczas rozmowy telefonicznej lub w postaci elektronicznej, jeżeli wynika to z przedmiotu usługi, jednak nie później niż w ciągu 3 dni roboczych od skierowania zapytania. Jeżeli nie jest możliwe wykonanie zadania w ciągu 3 dni roboczych, Wykonawca uzgodni z Zamawiającym inny termin konsultacji lub porady.

III.1.5 Pozostałe ustalenia

1. System Zgłoszeń, który zostanie udostępniony przez Wykonawcę, ma dodatkowo pozwalać na prowadzenie rejestru kontaktów z Zamawiającym obejmującego w szczególności wykonane czynności gwarancyjne, ewidencję wszystkich zgłoszeń gwarancyjnych, opis zmian w konfiguracji Oprogramowania; prowadzenie rejestru zgłoszeń jest obowiązkiem Wykonawcy.
2. Zamawiający przekaże Wykonawcy, zgodnie ze stanem swojej wiedzy, informacje o aktach prawa wewnętrznego obowiązującego w Podmiocie leczniczym, które mają zastosowanie w realizacji niniejszej Umowy.
3. Gwarancja i serwis na urządzenia muszą być świadczony przez firmę autoryzowaną przez producenta lub jego przedstawicielstwo w Polsce w przypadku, gdy Oferent nie posiada takiej autoryzacji.
4. Zamawiający ustala procedurę zdalnego dostępu Wykonawcy do Oprogramowania:
   1) Wykonawca drogą elektroniczną poprzez e-mail, prześle Zamawiającemu wniosek o uzyskanie zdalnego dostępu do Oprogramowania, wskazując co najmniej:
      a) imię i nazwisko pracownika Wykonawcy, któremu zostanie przyznany dostęp,
      b) nazwa i adres IP zasobu (bazy danych/oprogramowania), który zostanie udostępniony,
      c) usługi sieciowe, które zostaną udostępnione,
      d) okres czasu, na który będzie aktywowany dostęp,
      e) numer zgłoszenia gwarancyjnego,
      f) przyczyna złożenia wniosku,
      g) opis czynności, które zostaną wykonane,
      h) imię i nazwisko pracownika Wykonawcy uprawnionego do złożenia wniosku.
   2) Osoba wyznaczona przez Zamawiającego zaopiniuje wniosek i w formie elektronicznej poprzez e-mail odpowie, podając informację o zgodzie lub jej braku.
   3) Po zakończeniu prac Wykonawca ma obowiązek przesłać Zamawiającemu raport z wykonanych prac z wykorzystaniem zdalnego dostępu, podając czas ich trwania i zakres.
   4) Każdy zdalny dostęp do Oprogramowania musi być przez Wykonawcę odnotowany w Systemie Zgłoszeń,

5) Dostęp do zasobów Zamawiającego musi być zgodny z obowiązującą u niego polityką bezpieczeństwa. Zamawiający udostępni procedury bezpieczeństwa Wykonawcy, którego oferta zostanie wybrana jako najkorzystniejsza, po podpisaniu umowy.
6) W przypadku dostarczenia nowej lub zmodyfikowanej wersji Oprogramowania wymagającego aktualizacji lub wymiany Oprogramowania dostarczonego w ramach niniejszej Umowy, Wykonawca w ramach gwarancji ma obowiązek wymiany lub aktualizacji także tego Oprogramowania.

5. W ramach gwarancji Wykonawca zobowiązuje się do:

a) wykonywania modyfikacji bez wezwania lub na pisemne zgłoszenie Zamawiającego w celu dostosowania wszystkich elementów Oprogramowania RSI do obowiązujących przepisów prawnych,
b) przekazania Zamawiającemu informacji o nowych wersjach oprogramowania drogą elektroniczną na wskazany adres e-mail Zamawiającego,
c) udostępniania nowych wersji oprogramowania poprzez ustaloną witrynę internetową, w szczególności związanych z wejściem w życie nowych przepisów prawa lub zawierających nowe funkcjonalności, w szczególności związane z rozliczeniami z NFZ; w przypadku w którym udostępnianie następować będzie w związku ze zmianą przepisów prawa, Wykonawca zobowiązany będzie do udostępnienia nowej wersji oprogramowania na nie mniej niż 14 dni przed dniem wejścia w życie tych przepisów; udostępniania nowych wersji oprogramowania poprzez ustaloną witrynę internetową, w szczególności związanych z wejściem w życie nowych przepisów prawa lub zawierających nowe funkcjonalności, w szczególności związane z rozliczeniami z NFZ; w przypadku w którym udostępnianie następować będzie w związku ze zmianą przepisów prawa, Wykonawca zobowiązany będzie do jej dokonania na nie mniej niż 14 dni przed dniem wejścia w życie tych *przepisów,* a w przypadku, gdy przepisy te będą wchodziły w życie w terminie krótszym niż 14 dni od daty ich publikacji, w terminie nie później jak 14 dni od ich publikacji,
d) wysłania na adres korespondencyjny Zamawiającego nośnika CD/DVD lub Flash USB, zawierającego nową wersję oprogramowania, na pisemne żądanie wniesione przez Zamawiającego - każda nowa wersja musi posiadać unikalny numer;
e) wraz z nową wersją oprogramowania Wykonawca zobowiązany jest do przekazania nowej wersji Dokumentacji wraz z procedurą instalacji oprogramowania oraz informacją o parametryzacji i konfiguracji.
f) udzielanie konsultacji, porad, dodatkowej konfiguracji, tworzenia nowych raportów, wsparcia technicznego w zakresie wdrożenia oraz użytkowania oprogramowania RSI, przy czym:

- prace będą świadczone w dni robocze w godzinach od 8 do 16 w języku polskim, w siedzibie Zamawiającego lub za uzgodnieniem Stron, jako prace świadczone zdalnie
- tryb zgłaszania: telefonicznie, e-mail, faxem lub poprzez Elektroniczny System Zgłoszeń, konsultacje i porady będą udzielane na bieżąco podczas rozmowy telefonicznej lub w postaci elektronicznej, jednak nie później niż w ciągu 3 dni roboczych od skierowania zapytania. Jeżeli nie jest możliwe wykonanie zadania w ciągu 3 dni roboczych, Wykonawca uzgodni z Zamawiającym inny termin konsultacji lub porady, jeżeli Zamawiający wyrazi na to zgodę.

Uwaga:

W przypadku zapisu terminu, jako:

- Dzień Roboczy należy rozumieć każdy dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy.
- Godziny Robocze należy rozumieć godziny od 8.00 do 15.00 w każdym Dniu Roboczym.

W innych przypadkach należy rozumieć jako dzień kalendarzowy.