**Znak sprawy: EZ/ZP/206/2020/RI**

**Załącznik nr 1 do SIWZ**

**Szczegółowy Opis Przedmiotu Zamówienia**

**na Dostawę i Wdrożenie Infrastruktury Sprzętowej oraz Szpitalnego Systemu Informatycznego (SSI)**

Kielce 2020

Spis treści

[Rozdział I. Założenia początkowe oraz wymagania ogólne 3](#_Toc58242035)

[I.1 Wprowadzenie 3](#_Toc58242036)

[I.2 Cel projektu 3](#_Toc58242037)

[I.3 Integracja z centralnym systemem e-zdrowie 4](#_Toc58242038)

[I.4 Akty prawne 6](#_Toc58242039)

[I.5 Ogólny opis przedmiot zamówienia 6](#_Toc58242040)

[I.6 Termin realizacji Przedmiotu Zamówienia 9](#_Toc58242041)

[I.7 Organizacja wdrożenia 10](#_Toc58242042)

[I.7.1 Założenia podstawowe 10](#_Toc58242043)

[I.7.2 Przygotowanie Dokumentacji 11](#_Toc58242044)

[I.7.3 Harmonogram wdrożenia 12](#_Toc58242045)

[I.7.4 Analiza Przedwdrożeniowa 12](#_Toc58242046)

[I.7.5 Dokumentacja Powykonawcza 14](#_Toc58242047)

[I.7.6 Odbiór 18](#_Toc58242048)

[I.7.7 Dostawa i instalacja oprogramowania standardowego 18](#_Toc58242049)

[I.7.8 Dostawa, instalacja, konfiguracja i wdrożenie Oprogramowania aplikacyjnego 19](#_Toc58242050)

[I.7.9 Testy 19](#_Toc58242051)

[I.7.10 Dodatkowe zobowiązania Wykonawcy 20](#_Toc58242052)

[Rozdział II. Szczegółowy opis przedmiotu zamówienia 21](#_Toc58242053)

[II.1 Dostawa i wdrożenie oprogramowania i Infrastruktury Serwerowej 21](#_Toc58242054)

[II.1.1 Serwer wirtualizacyjny 24](#_Toc58242055)

[II.1.2 Serwer do kopii (backup) 26](#_Toc58242056)

[II.1.3 Serwer bazodanowy 29](#_Toc58242057)

[II.1.4 Serwer bazodanowy zapasowy 31](#_Toc58242058)

[II.1.5 Macierz główna 33](#_Toc58242059)

[II.1.6 Macierz zapasowa 37](#_Toc58242060)

[II.1.7 Macierz backup/serwer 40](#_Toc58242061)

[II.1.8 Biblioteka LTO 42](#_Toc58242062)

[II.1.9 Przełącznik zasobowy do macierzy 43](#_Toc58242063)

[II.1.10 Szafa rack 45](#_Toc58242064)

[II.1.11 Zasilacz awaryjny UPS 46](#_Toc58242065)

[II.2 Oprogramowanie systemowe i narzędziowe 48](#_Toc58242066)

[II.2.1 Serwerowy system operacyjny 48](#_Toc58242067)

[II.2.2 Licencje dostępowe serwera 51](#_Toc58242068)

[II.2.3 Oprogramowanie bazodanowe 53](#_Toc58242069)

[II.2.4 Oprogramowanie systemowe storage 55](#_Toc58242070)

[II.2.5 Oprogramowanie systemowe Load Balancer 57](#_Toc58242071)

[II.2.6 Oprogramowanie wirtualizacyjne 60](#_Toc58242072)

[II.2.7 Oprogramowanie do robienia kopii zapasowych 63](#_Toc58242073)

[II.3 Modernizacja sieci LAN w zakresie dostawy i wdrożenia aktywnych urządzeń sieciowych 64](#_Toc58242074)

[II.3.1 Przełącznik LAN - Przełącznik zarządzający 65](#_Toc58242075)

[II.3.2 Przełącznik LAN - Przełącznik rdzeniowy 66](#_Toc58242076)

[II.3.3 Przełącznik LAN - Przełącznik dostępowy 69](#_Toc58242077)

[II.4 Dostawa i wdrożenie Szpitalnego Systemu Informatycznego SSI 71](#_Toc58242078)

[II.4.1 Wymogi dotyczące interoperacyjności lub migracji dla oferowanego SSI 71](#_Toc58242079)

[II.4.2 Dostępność dostarczanego rozwiązania 72](#_Toc58242080)

[II.4.3 Wymagany stan docelowy 73](#_Toc58242081)

[II.4.4 Oprogramowanie aplikacyjne – wymagania ogólne 74](#_Toc58242082)

[II.4.5 Szpitalny System Informatyczny – wymagania szczegółowe 79](#_Toc58242083)

[II.4.6 Migracja danych 94](#_Toc58242084)

[II.4.7 Warunki przeniesienia danych 96](#_Toc58242085)

[II.4.8 Instruktaże stanowiskowe 97](#_Toc58242086)

[Rozdział III. Gwarancja 100](#_Toc58242087)

[III.1.1 Zakres usług gwarancyjnych dostarczonego oprogramowania aplikacyjnego. 102](#_Toc58242088)

[III.1.2 Usługi gwarancyjne 103](#_Toc58242089)

[III.1.3 Pozostałe ustalenia: 110](#_Toc58242090)

# Założenia początkowe oraz wymagania ogólne

## Wprowadzenie

W projekcie „Informatyzacja Placówek Medycznych Województwa Świętokrzyskiego (InPlaMed WŚ), w ramach Regionalnego Programu Operacyjnego Województwa Świętokrzyskiego na lata 2014-2020 (RPOWŚ 2007-2014)”, bierze udział Województwo Świętokrzyskie - będące Liderem Projektu, w imieniu którego zadania realizowane są przez Urząd Marszałkowski Województwa Świętokrzyskiego i 8 podmiotów leczniczych jednostek organizacyjnych Województwa oraz 12 podmiotów leczniczych będących jednostkami organizacyjnymi powiatów.

## Cel projektu

Głównym celem Projektu „Informatyzacja Placówek Medycznych Województwa Świętokrzyskiego” jest wdrożenie Elektronicznej Dokumentacji Medycznej (EDM) w placówkach medycznych objętych projektem, z zastosowaniem rozwiązań technologicznych i organizacyjnych zapewniających ciągłość działania oraz zgodność z regulacjami i wymogami prawnymi, protokołami przyjętymi w ochronie zdrowia, a także wytycznymi Centrum Systemów Informacyjnych Ochrony Zdrowia, jako instytucji państwowej, której zadaniem jest budowa oraz wspieranie i monitorowanie procesów budowy systemów informacyjnych w ochronie zdrowia. Cel ten przekłada się na usprawnienie zarządzania i podniesienie jakości procesów leczniczych.

Ponadto zakłada się budowę usług elektronicznych w obszarze ochrony zdrowia, świadczonych w ramach poszczególnych placówek medycznych biorących udział w projekcie oraz całego regionu, na rzecz pacjentów oraz personelu medycznego, w jak najszerszym możliwym do realizacji pod względem finansowym, organizacyjnym i prawnym zakresie.

Kluczową usługą budowaną w ramach Projektu będzie gromadzenie i udostępnianie Elektronicznej Dokumentacji Medycznej (EDM) w sposób zapewniający nienaruszalność i bezpieczeństwo przechowywania danych w długim okresie czasu, przy jednoczesnym zapewnieniu łatwego dostępu dla wszystkich uprawnionych użytkowników oraz zachowaniu wysokiej wydajności działania.

Zakłada się osiągnięcie celów Projektu poprzez rozbudowę i rozszerzenie aktualnego stanu informatyzacji poszczególnych placówek medycznych uczestniczących w projekcie z możliwością w przyszłości rozbudowy o kolejne e-usługi i funkcjonalności, w tym także budowę integracyjnej warstwy regionalnej.

Zakres rozbudowy i rozszerzenia aktualnego stanu informatyzacji poszczególnych placówek medycznych został w ramach projektu zaktualizowany indywidualnie dla poszczególnych placówek medycznych uczestniczących w projekcie na podstawie analizy stanu aktualnego. W ramach projektu zakładane jest - w zależności od indywidualnych potrzeb placówek medycznych - zarówno dostarczenie wymaganych w ramach projektu funkcjonalności biznesowych realizowanych poprzez dostawę nowych systemów dziedzinowych (lub dostosowanie i integrację zastanych medycznych systemów dziedzinowych) oraz lokalnych repozytoriów EDM. Przewidywana jest także rozbudowa warstwy infrastrukturalno–systemowej poprzez dostawę komponentów i rozwiązań w obszarze sieciowym, sprzętowym oraz oprogramowania systemowego.

## Integracja z centralnym systemem e-zdrowie

Dostarczony Szpitalny System Informatyczny (SSI) musi zapewnić integrację funkcjonalną z systemem teleinformatycznym, o którym mowa w art. 7 ust. 1 ustawy o systemie informacji w ochronie zdrowia (tj. Dz.U. z 2017 roku, poz. 1845 z poźn. zm), co najmniej w zakresie opisanym w dokumentach: „Opis usług biznesowych Systemu P1 wykorzystywanych w systemach usługodawców”, „Opis funkcjonalny Systemu P1 z perspektywy integracji systemów zewnętrznych” opublikowanych przez CSIOZ oraz „Minimalne wymagania dla systemów usługodawców (<https://www.gov.pl/web/zdrowie/minimalne-wymagania-dla-systemow-uslugodawcow>) oraz dokumentacja integracyjna dla obszaru Zdarzeń Medycznych i Indeksów EDM.

W zakresie integracji i komplementarności z centralnymi systemami e-zdrowia, na Wykonawcy będzie spoczywał obowiązek dostosowania zaoferowanego rozwiązania do wymagań ujętych w dokumentach publikowanych poprzez CSIOZ, w tym w szczególności do:

* Zakresu funkcjonalnego Projektu P1 (system musi posiadać m.in. możliwość wystawiania recept elektronicznych oraz skierowań elektronicznych),
* Opisu funkcjonalnego Systemu P1 z perspektywy integracji systemów zewnętrznych,
* Dokumenty te dostępne są na stronie internetowej CSIOZ, pod adresem: http://csioz.gov.pl.
* Wykonawca zobowiązany jest do zapewnienia integracji z węzłem krajowym identyfikacji elektronicznej. Wykonawca zobowiązany jest do dostarczenia puli licencji niezbędnych do integracji z węzłem krajowym w zakresie poprawnego działania całego przedmiotu zamówienia.

W zakresie integralności zaoferowanego Szpitalnego Systemu Informatycznego Wykonawca powinien uwzględnić i w razie obowiązującego wymogu wdrożyć poniższe wytyczne i założenia:

* System P1 dostępny będzie dla odpowiednio zarejestrowanych w CSIOZ 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 CSIOZ.
* Komunikaty przesyłane do P1 powinny być podpisane 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-zdrowia.
* W przypadku informacji o zdarzeniu medycznym – obowiązuje Model Informacji o Zdarzeniu Medycznym i Indeksie Dokumentacji Medycznej (dalej: EDMiZM) publikowany przez CSIOZ.
* W przypadku rejestru (indeksu) Elektronicznej Dokumentacji Medycznej – obowiązuje EDMiZM publikowany przez CSIOZ.
* 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 CSIOZ.
* 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 CSIOZ.

Jednocześnie, zaoferowany Szpitalny System Informatyczny powinien spełniać następujące założenia funkcjonalne:

* Prowadzenie i wymiana Elektronicznej Dokumentacji Medycznej (EDM), w tym indywidualnej dokumentacji medycznej (wewnętrznej i zewnętrznej), uwzględniać musi rozwiązania umożliwiające zbieranie przez podmiot udzielający świadczeń opieki zdrowotnej jednostkowych danych medycznych w elektronicznym rekordzie pacjenta oraz tworzenie EDM zgodnej co najmniej ze standardem HL7 CDA, opracowanym i opublikowanym przez CSIOZ – Polską Implementacją Krajową HL7 CDA (tzw. IG).
* Szpitalny System Informatyczny powinien uwzględniać funkcjonalności dotyczące prowadzenia repozytorium EDM (z obsługą przechowywania EDM) oraz uwzględniać rozwiązania zapewniające wymianę EDM pomiędzy repozytorium Zamawiającego, a Platformą P1. Platforma P1 będzie zawierała katalog EDM, w którym znajdować się będą informacje o EDM tworzonym i przechowywanym u Zamawiającego.
* Repozytorium EDM powinno 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.

## 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.).

## Ogólny opis przedmiot zamówienia

Przedmiot zamówienia niniejszego postępowania przetargowego obejmuje dostawę i wdrożenie Infrastruktury Serwerowej i Sieciowej oraz Szpitalnego Systemu Informatycznego (SSI).

1. **dostawę i wdrożenie Infrastruktury Serwerowej wraz z oprogramowaniem systemowym i narzędziowym:**
* Infrastruktura serwerowa w zakresie:

|  |  |  |
| --- | --- | --- |
| **Poz. SOPZ** | **Opis** | **Ilość**  |
| **Rozdział II.1** | **Infrastruktura serwerowa**  |   |
| II.1.1 | Serwer wirtualizacyjny | 4 szt. |
| II.1.2 | Serwer do kopii (backup) | 1 szt. |
| II.1.3 | Serwer bazodanowy | 1 szt. |
| II.1.4 | Serwer bazodanowy zapasowy | 1 szt. |
| II.1.5 | Macierz główna | 1 szt. |
| II.1.6 | Macierz zapasowa | 1 szt. |
| II.1.7 | Macierz backup/serwer | 1 szt. |
| II.1.8 | Biblioteka LTO | 1 szt. |
| II.1.9 | Przełącznik zasobowy do macierzy | 4 szt. |
| II.1.10 | Szafa rack | 1 szt. |
| II.1.11 | Zasilacz awaryjny UPS | 3 szt. |

* Oprogramowanie systemowe i narzędziowe w zakresie:

|  |  |  |
| --- | --- | --- |
| **Poz. SOPZ** | **Opis** | **Ilość**  |
| **Rozdział II.2** | **Oprogramowanie systemowe i narzędziowe** |   |
| II.2.1 | Serwerowy system operacyjny | 4 szt. |
| II.2.2 | Licencje dostępowe serwera | 500 szt. |
| II.2.3 | Oprogramowanie bazodanowe | 1 szt. |
| II.2.4 | Oprogramowanie systemowe storage | 24 szt. |
| II.2.5 | Oprogramowanie systemowe Load Balancer | 2 szt. |
| II.2.6 | Oprogramowanie wirtualizacyjne | 1 szt. |
| II.2.7 | Oprogramowanie do robienia kopii zapasowych | 1 szt. |

1. **modernizacja sieci LAN w zakresie dostawy i wdrożenia sieciowej infrastruktury sprzętowej:**

|  |  |  |
| --- | --- | --- |
| **Poz. SOPZ** | **Opis** | **Ilość** |
| **Rozdział II.3** | **Modernizacja sieci LAN** |  |
| **AKTYWNE URZĄDZENIA SIECIOWE** |
| Przełącznik LAN | 1 kpl. |
| II.3.1 | Przełącznik zarządzający | 3 szt. |
| II.3.2 | Przełącznik rdzeniowy | 2 szt. |
| II.3.3 | Przełącznik dostępowy | 5 szt. |

1. **dostawa i wdrożenie Szpitalnego Systemu Informatycznego SSI**:

|  |  |
| --- | --- |
| **Poz. SOPZ** | **Opis** |
| **Rozdział II.4** | **Szpitalny System Informatyczny** |
| II.4.5   | System HIS – część medyczna – dostawa i wdrożenie |
| System LIS – integracja z HIS |
| Elektroniczna Dokumentacja Medyczna – dostawa i wdrożenie |
| e-Usługi – eRejestracja On-Line z Portalem – dostawa i wdrożenie |
| II.4.8 | Instruktaże stanowiskowe |

1. Przedmiot zamówienia musi być dostarczany, wdrożony i zainstalowany w całości do siedziby Zamawiającego.
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).
* 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.
1. Usługi projektowania, instalacji, konfiguracji i wdrożenia Wykonawca przeprowadzi zgodnie
z zapisami niniejszego SOPZ w uzgodnieniu z Zamawiającym, zgodnie z obowiązującymi przepisami, zasadami wykonywania projektów teleinformatycznych oraz najlepszymi praktykami w ich realizacji.
2. Wykonawca jest zobowiązany do realizacji Przedmiotu Zamówienia zgodnie z zasadami i wytycznymi Zamawiającego, zapisami SOPZ oraz Umowy.
3. Ilekroć w niniejszym SOPZ Zamawiający użył w opisie oznaczeń norm, aprobat, specyfikacji technicznych i systemów odniesienia, o których mowa w art. 30 ust. 1-3 Pzp należy je rozumieć jako przykładowe. Zamawiający zgodnie z art. 30 ust. 4 ustawy Pzp dopuszcza produkty równoważne opisywanym w treści SIWZ. Jeżeli zapisy zawarte w niniejszym załaczniku wskazywałyby w odniesieniu do rozwiązań, materiałów lub urządzeń znaki towarowe lub pochodzenie Zamawiający, zgodnie z art. 29 ust. 3 ustawy PZP, dopuszcza składanie ofert na „produkty” równoważne. 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. Zamawiający, przy opisie przedmiotu zamówienia, wskazując oznaczenie konkretnego producenta (dostawcy) lub konkretny produkt, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych, co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych parametrach lub lepszych. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów, wykazujących spełnienie przez produkty równoważne ww. parametrów i cech.
4. 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.
5. Zamawiający wymaga, aby zaoferowane rozwiązanie (system) było rozwiązaniem istniejącym, działającym, gotowym do wdrożenia i zapewniającym realizację wszystkich wymaganych w SIWZ
(w szczególności SOPZ) funkcjonalności na dzień składania ofert i nie może być w fazie opracowywania, budowy, testów, projektowania itp.
6. Wszelkie dostarczane urządzenia:
* Muszą być fabrycznie nowe, pochodzić z autoryzowanego kanału sprzedaży producenta
i reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się urządzeń: odnawianych, demonstracyjnych lub powystawowych.
* Nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta.
* Elementy, z których zbudowane są urządzenia muszą być produktami producenta urządzeń lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta.
* Urządzenia i ich komponenty muszą być oznakowane w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
* Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach producenta.
* Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w języku polskim lub angielskim w formie papierowej lub elektronicznej.
* Urządzenia na etapie dostawy producent, a zamawiający nie mogą podlegać modyfikacjom.

## Termin realizacji Przedmiotu Zamówienia

Termin realizacji całości Przedmiotu zamówienia wynosi **180 dni** od dnia podpisania Umowy.

## Organizacja wdrożenia

### 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.
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. Zamawiający przewiduje częstotliwość narad maksymalnie 1 raz w miesiącu, chyba że, nadzwyczajna sytuacja w realizacji przedmiotu umowy wymagała będzie częstszych spotkań.
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 przygotuje informacje na temat struktury organizacyjnej Zespołu Wykonawcy zajmującą 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, w punktach muszą realizować osoby wymienione w ofercie Wykonawcy, przy czym:
	1. Osoby Zespołu Wykonawcy muszą być dyspozycyjne w trakcie wykonywania prac,
	2. Wykonawca przekaże Zamawiającemu wykaz numerów telefonów kontaktowych do kluczowych osób biorących udział w realizacji Przedmiotu Zamówienia po stronie Wykonawcy,
11. Wykonawca zorganizuje prace tak, aby w maksymalnym stopniu nie zakłócać ciągłości funkcjonowania prac u Zamawiającego.
12. Obiekty podlegające inwestycji (obiekty służby zdrowia w których świadczone są usługi medyczne) 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 medycznych.
13. Wykonawca musi uwzględnić, że wszystkie prace wykonywane będą w użytkowanych obiektach przy dużym ruchu pracowników i chorych, tzn. organizacja prac powinna przede wszystkim zapewniać bezpieczeństwo przebywających w oddziałach pracowników i chorych oraz zachowanie ciszy nocnej w godzinach właściwych dla Zamawiającego.

### Przygotowanie Dokumentacji

1. W ramach procesu prac Wykonawca opracuje dla Zamawiającego Dokumentację Przedmiotu Zamówienia(zwaną dalej Dokumentacją), która składa się z nw. zakresów:
2. Harmonogram Wdrożenia.
3. Dokumentacja Analizy Przedwdrożeniowej (DAP).
4. Dokumentacja Powykonawcza.
5. Dokumentacja powyższa będzie 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 Specyfikacją Istotnych Warunków Zamówienia wraz z załącznikami (dalej zwanych SIWZ) będę stanowiły podstawę do weryfikacji wdrożenia w trakcie odbiorów.
6. Dokumentacja podlega uzgadnianiu i akceptacji Zamawiającego. Akceptacja Harmonogramu wdrożenia i DAP warunkuje rozpoczęcie prac Wykonawcy.
7. Dokumentacja Analizy Przedwdrożeniowej DAP wraz z Harmonogramem wdrożenia zostaną opracowane w oparciu o wymagania określone w niniejszym SOPZ.

### Harmonogram wdrożenia

Wykonawca zobowiązany jest opracować na podstawie SIWZ oraz SOPZ szczegółowy harmonogram wdrożenia. Harmonogram należy przedstawić Zamawiającemu w terminie do 21 dni od podpisania Umowy.

### Analiza Przedwdrożeniowa

1. Analiza przedwdrożeniowa, którą należy rozumieć jako zakres czynności do wykonania przez Wykonawcę mający 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 będzie realizowany organizacyjnie i technicznie Przedmiot Zamówienia. Dokumentacja Analizy Przedwdrożeniowej będzie podlegała uzgodnieniu i akceptacji Zamawiającego.
2. Dokumentacja Analizy Przedwdrożeniowej DAP powinna zawierać w szczególności:

|  |
| --- |
| **Zawarość DAP** |
| **SSI** |
| * wykaz oraz szczegółowy opis i harmonogram wdrożenia SSI i e-usług
 |
| * architekturę SSI i e-usług
 |
| * analizę migracji danych oraz opis sposobu migracji – jeżeli dotyczy
 |
| * przygotowanie planu instalacji Infrastruktury serwerowej z uwzględnieniem rozmieszczenia sprzętu w lokalizacjach Zamawiającego
 |
| * przygotowanie planu instalacji macierzy dyskowych
 |
| * jednoznacznie określone założenia integracji z innymi systemami informatycznymi, które posiada Zamawiający
 |
| * plan pracy na dalsze etapy Wdrożenia
 |
| * plan migracji danych z SSI, który posiada Zamawiający – jeżeli dotyczy
 |
| * szczegółową specyfikację oprogramowania objętego zakresem umowy
 |
| * wykaz oraz szczegółowy opis i harmonogram niezbędnych prac konfiguracyjnych
 |
| * ustawienia konfiguracyjne urządzeń i oprogramowania wchodzących w skład SSI
 |
| * 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
 |
| * harmonogram instruktażu personelu oraz administratorów SSI
 |
| **Zarządcze** |
| * plan i sposób komunikacji Stron
 |
| **Infrastruktura Serwerowa** |
| * podział Przedmiotu Zamówienia na Produkty, a następnie ich pogrupowanie w Komponenty
 |
| * analizę wymagań Przedmiotu Zamówienia zawierającą opis sposobu realizacji wymagań, sposób testowania i odbioru
 |
| * karty katalogowe urządzeń potwierdzające spełnienie wymagań
 |
| * plan dostaw
 |
| * opis instalacji i wdrożenia oprogramowania wdrażanego wraz z Infrastrukturą serwerową
 |
| * opis modernizacji i budowy Infrastruktury serwerowej,
 |
| * lista Komponentów, które będę podlegały osobnym odbiorom – jeżeli dotyczy
 |
| * szczegółowy zakres i zawartość pozostałej Dokumentacji
 |
| **Infrastruktura Sieciowa** |
| * podział Przedmiotu Zamówienia na Produkty, a następnie ich pogrupowanie w Komponenty
 |
| * analizę wymagań Przedmiotu Zamówienia zawierającą opis sposobu realizacji wymagań, sposób testowania i odbioru
 |
| * karty katalogowe urządzeń potwierdzające spełnienie wymagań
 |
| * dokumentację i plan dostaw
 |
| * Plan, opis instalacji i wdrożenia oprogramowania wdrażanego wraz z aktywną Infrastrukturą sieciową
 |
| * listę Komponentów, które będę podlegały osobnym odbiorom – jeżeli dotyczy
 |
| * szczegółowe uzgodnienia Stron Umowy dotyczące zakresu i sposobu integracji dostarczanych rozwiązań z istniejącą infrastrukturą u Zamawiającego
 |
| * zakres prac realizowanych przez podwykonawców,
 |
| * szczegółowy zakres i zawartość pozostałej Dokumentacji
 |

### 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.
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 powinna zawierać:

#### Wymogi ogólne:

1. Pełna charakterystyka licencjonowania wszystkich elementów aplikacji i środowiska.
2. 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),
	* dla komponentów innych dostawców, należy dokładnie określić wykorzystywane i dopuszczalne wersje;
3. Konfiguracja musi obejmować wszystkie urządzenia wdrożone, zainstalowane w ramach budowy systemu IT.
4. 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.,
	* infrastrukturę sieciową– parametry sprzętowe (porty fibre channel, aktywne licencje, itp.), fabric, zonning, aliasy, itp.;
5. Opis architektury logicznej:
* schemat i opis powiązań logicznych poszczególnych komponentów i ich rolę w architekturze.
1. Mapa 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.
1. 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.
1. Dokumentacja administracyjna związana 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,
2. Dokumenty z testów:
* plan testów, scenariusze testowe i protokoły z testów akceptacyjnych, wydajnościowych, testów operacji administratora technicznego oraz testów bezpieczeństwa w tym ciągłości działania (przełączanie, odtwarzanie, weryfikacja poprawności).
1. Dokumentacja wdrożeniowa:
	* 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.
2. Wersjonowanie:
* opis zasad wersjonowania i sposobu patchowania aplikacji.
1. Zalecenia:
* opis zasad i zaleceń strojenia aplikacji.
1. Instrukcje obsługi i instrukcje użytkowania dla wersji dostarczonego oprogramowania z podziałem na poszczególne moduły.
2. W zakresie obszarów administratora dokumentacja powinna 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 SSI lub/i e-usług;
	* opis zarządzania autoryzacją i autentykacją użytkowników
3. Wkład do Polityki bezpieczeństwa w zakresie wdrożonego Systemu oraz Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych opracowane zgodnie
z wymaganiami określonymi w R[ozporządzeniu 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)](https://uodo.gov.pl/pl/131/224). Wkład do Polityki Bezpieczeństwa będzie 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.

#### Wymogi szczegółowe:

1. 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.
2. Procedury tworzenia środowisk pomocniczych.
* zasady i procedury tworzenia środowisk (testowych, rozwojowych, raportowych) oraz metod klonowania i anonimizacji (depersonifikacji) danych przenoszonych pomiędzy środowiskami;
1. Procedury eksploatacji.
	* w szczególności dokumentacja zawiera 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.),
	* 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 obejmują również procedury i instrukcje instalacji krok po kroku środowiska produkcyjnego „od podstaw” na:
		+ 1. środowisku fizycznych hostów danego Zamawiającego rozpoczynając od dostarczonego wirtualizatora,
			2. standardowym zastosowanym systemie operacyjnym dla poszczególnych dostarczonych systemów informatycznych.
2. Po skonfigurowaniu urządzeń sieciowych oraz podłączeniu hostów do sieci komputerowej należy również sporządzić dokumentację powykonawczą logicznej struktury sieci. Dokumentacja powykonawcza powinna zawierać co najmniej:

|  |
| --- |
| **Dokumentacja Powykonawcza logicznej struktury sieci** |
| * Informacje ogólne
 |
| * Opis sposobu i struktury adresacji logicznej sieci
 |
| * Schemat logicznej struktury sieci
 |

1. 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.

### Odbiór

1. Odbiór końcowy Przedmiotu Zamówienia ma na celu potwierdzenie wykonania wszystkich zadań wynikających z Umowy oraz dostarczenia wymaganej zamówieniem Dokumentacji.
2. Odbiory będą odbywać się zgodnie z zapisami w Umowie stanowiącej Dodatek nr 4 do SIWZ.

### 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 Dodatek nr 4 do SWIZ oraz w istniejących systemach informatycznych zgodnie z wymaganiami niniejszego Szczegółowego 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.

### Dostawa, instalacja, konfiguracja i wdrożenie Oprogramowania aplikacyjnego

1. Zadanie dostawy, instalacji, konfiguracji i wdrożenia Oprogramowania aplikacyjnego obejmuje:
	1. SSI (HIS, LIS),
	2. E-usługi.
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 SIWZ oraz zgodnie z Dokumentacją i wskazanymi przez Zamawiającego wytycznymi na etapie analizy przedwdrożeniowej oraz oczekiwaniami konfiguracyjnymi samego procesu wdrażania (w zakresie opisanych w SOPZ 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 przewiduje konieczność przeprowadzenia przez Wykonawcę migracji dotychczasowego środowiska SSI na platformę sprzętową dostarczaną w ramach przedmiotu zamówienia. Wykonawca ponosi pełną odpowiedzialność za migrowane środowiska oraz zgromadzone dane.
6. Zamawiający na potrzeby realizacji przedmiotu zamówienia przewidział infrastrukturę serwerową i oprogramowanie o parametrach wskazanych w rozdziale II niniejszego SOPZ.

### Testy

1. W ramach postępowania zostaną 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.

### Dodatkowe zobowiązania Wykonawcy

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

# Szczegółowy opis przedmiotu zamówienia

## Dostawa i wdrożenie oprogramowania i 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 Szpitalnego Systemu Informatycznego i e-usług.
2. Jeżeli zajdzie potrzeba, wraz z dostarczaną 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 (Systemu Komunikacyjnego) Zamawiającego.
3. Wykonawca jest zobowiązany dokonać montażu dostarczonej Infrastruktury Serwerowej oraz oprogramowania w miejscach wskazanych przez Zamawiającego.
4. Wszystkie elementy Infrastruktury serwerowej powinny zostać zamontowane w zakupywanej szafie serwerowej rack oraz innych udostępnionych przez Zamawiającego szafach rack, w sposób umożliwiający ich prawidłową wentylację.
5. Wszystkie urządzenia muszą być fabrycznie nowe wyprodukowane po dniu 1 stycznia 2020r.
6. Szczegóły dotyczące instalacji i uruchomienia Infrastruktury serwerowej zostaną ustalone w trakcie Analizy Przedwdrożeniowej.
7. W zakresie części serwerowej w ramach postępowania wymagane jest wykonanie następujących usług:
	* + - Instalacja fizyczna dostarczonej Infrastruktury
				* Przygotowanie planu instalacji:
* Zestawienie dostarczanych urządzeń
* Propozycję rozmieszczenia elementów w istniejących szafach rackowych oraz innych udostępnionych przez Zamawiającego szafach rack
* Propozycję testów odbiorczych
	+ - * + Instalacja, montaż i uruchomienie serwerów wirtualizacyjnych:
* Montaż serwera w istniejącej szafie rackowej oraz innych udostępnionych przez Zamawiającego szafach rack
* Podłączenie serwera do sieci LAN i/lub SAN
* Podłączenie serwera do zasilania
* Inicjalne uruchomienie serwera
* Testy działania serwera oraz weryfikacja parametrów
	+ - * + Instalacja, montaż i uruchomienie infrastruktury backupowej:
* Montaż urządzeń w istniejącej szafie rackowej
* Podłączenie urządzeń do sieci LAN i/lub SAN
* Podłączenie urządzeń do zasilania
* Podłączenie biblioteki taśmowej do serwera backupu/systemu pamięci masowej
* Aktualizacja oprogramowania do najnowszej stabilnej wersji
* Inicjalne uruchomienie urządzeń
* Testy działania oraz weryfikacja parametrów
	+ - * + Instalacja, montaż i uruchomienie macierzy dyskowych:
* Montaż macierzy w szafie rackowej
* Podłączenie macierzy do sieci LAN i/lub SAN
* Inicjalne uruchomienie macierzy
* Testy działania macierzy oraz weryfikacja parametrów
	+ - * Konfiguracja macierzy dyskowych
				+ 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
	+ - * + Implementacja zgodna z projektem:
* Instalacja sprzętowa
* Aktywacja zakupionego oprogramowania
* Konfiguracja replikacji
* Implementacja zaakceptowanej konfiguracji logicznej macierzy
	+ - * + Testy odbiorcze:
* Zestawienie stosowanej nomenklatury
* Weryfikację zgodności z planem wdrożenia
* Przeprowadzenie testów potwierdzających poprawność instalacji macierzy
	+ - * + 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
	+ - * Instalacja oprogramowania wirtualizacyjnego i backupowego
				+ Inwentaryzacja stanu obecnego:
* Zestawienie nazewnictwa poszczególnych elementów istniejącego systemu
* Zestawienie zainstalowanych łat systemu operacyjnego
* Zestawienie zainstalowanych wersji oprogramowania
	+ - * + Przygotowanie projektu technicznego:
* Zestawienie stosowanej nomenklatury
* Rysunki logicznej struktury systemu
* Propozycję nazewnictwa poszczególnych elementów systemu wirtualizacji i backupu.
* Zestawienie wymaganych łat systemu operacyjnego (ang. Patch Management)
* Zestawienie wymaganych wersji oprogramowania
* Propozycje konfiguracji systemu wirtualizacji i backupu
	+ - * + Implementacja zgodna z projektem:
* Instalacja oprogramowania wirtualizacyjnego i backupowego
* Konfiguracja oprogramowania wirtualizacyjnego i backupowego
* Aktywacja dostarczonego oprogramowania
	+ - * + Przygotowanie dokumentacji powykonawczej. Winna zawierać:
* Zestawienie stosowanej nomenklatury
* Rysunki logicznej struktury systemu wirtualizacji i backupu
* Zestawienie nazewnictwa poszczególnych elementów systemu
* Zestawienie konfiguracji systemu wirtualizacji
* Zestawienie zainstalowanych łat systemu operacyjnego (ang. Patch Management)
* Zestawienie wersji zainstalowanego oprogramowania
1. 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 nabycia dla Zamawiającego licencji (nie dotyczy samego systemu SSI) oraz nośnikami danych zawierającymi zainstalowane oprogramowanie (o ile dostarcza je producent). 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 zewnętrzną, w środowisku Zamawiającego.
2. Wykonawca zobowiązany jest zapewnić 6 miesięczną możliwość prowadzenia konsultacji w zakresie administracji zaoferowanym sprzętem oraz dostarczonym oprogramowaniem narzędziowym (systemowym, wirtualizacyjnym, backup-owym i bazodanowym) z osobami wskazanymi przez Wykonawcę w ilości nie większej niż 50 godzin.

### Serwer wirtualizacyjny

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

|  |  |
| --- | --- |
| **Cecha** | **Wymagania minimalne** |
| Obudowa | Obudowa Rack o wysokości max 2U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. |
| Płyta główna | Płyta główna z możliwością zainstalowasatania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
| Chipset | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |
| Procesor | Zainstalowane dwa procesory ośmiordzeniowe x86 min. **3.3GHz** umożliwiające osiągnięcie wyniku **min. 120** w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów. |
| RAM | * 768GB RDIMM 2666MT/s, na płycie głównej powinny znajdować się minimum 24 sloty przeznaczone do rozbudowy pamięci.
* Płyta główna powinna obsługiwać do min. 3TB pamięci RAM.
 |
| Zabezpieczenia pamięci RAM | Memory Rank Sparing, Memory Mirror |
| Gniazda PCI | Min. Pięć slotów PCIe Gen 3 w tym dwa sloty PCIe Gen 3 o prędkości min. x16. |
| Interfejsy sieciowe/FC/SAS | Wbudowane lub dołożone dwie karty dwuportowe 10GbE SFP+. Karty dostarczyć wraz z wkładkami 10GBASE-LR lub SR. Patchcordy odpowiedniego typu o wymaganej długości. Zastosowanie do połączenia serwera z przełącznikiem w szafie.Dwie karty jednoportowe FC 16Gb HBA |
| Dyski twarde | Możliwość instalacji dysków SATA, SAS, SSD. Zainstalowany dedykowany moduł dla hypervisora wirtualizacyjnego, wyposażony w nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. |
| Wbudowane porty | * min. 1 port USB 2.0 oraz 2 porty USB 3.0,
* 2 porty video (1 na przednim panelu obudowy, drugi na tylnym)
 |
| Video | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1440 x 900 |
| Wentylatory | Redundantne |
| Zasilacze | Redundantne, Hot-Plug o mocy co najmniej 700W każdy z dedykowanymi przewodami zasilającymi. Wykonawca powinien dopasować moc zasilaczy do zaproponowanej konfiguracji serwera.  |
| Bezpieczeństwo | Płyta wyposażona w moduł TPM.  |
| Diagnostyka | Wbudowany panel LCD lub umieszczony na panelu zabezpieczającym lub diody umieszczone na froncie obudowy. |
| Karta Zarządzania | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:* zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
* zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
* szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;
* możliwość podmontowania zdalnych wirtualnych napędów;
* wirtualną konsolę z dostępem do myszy, klawiatury;
* wsparcie dla Ipv6;
* SNMP; IPMI2.0, SSH, Redfish;
* możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;
* możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;
* integracja z Active Directory;
* możliwość obsługi przez dwóch administratorów jednocześnie;
* wsparcie dla dynamic DNS;
* wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
 |
| Certyfikaty | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001
* Serwer musi posiadać deklaracja CE
* Serwer musi posiadać wsparcie dla oferowanego systemu wirtualizacyjnego
 |
| Dokumentacja użytkownika | * Dokumentacji w języku polskim lub angi*e*lskim.
 |

### Serwer do kopii (backup)

Wymagane dostarczenie jest 1 szt. serwera spełniającego poniżej opisane minimalne parametry funkcjonalne:

|  |  |
| --- | --- |
| **Cecha** | **Wymagania minimalne** |
| Obudowa | Obudowa Rack o wysokości max 2U z możliwością instalacji do 12 dysków 3.5” Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych |
| Płyta główna | Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
| Chipset | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. |
| Procesor | Zainstalowane dwa procesory ośmiordzeniowe klasy x86, dedykowane do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. **80** w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów. |
| RAM | 96GB RDIMM 2666MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 512Gb pamięci RAM. |
| Zabezpieczenia pamięci RAM | Memory Rank Sparing, Memory Mirror |
| Interfejsy sieciowe/FC/SAS | Wbudowane dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseTDodatkowo zainstalowane karty:* karta dwuportowa 10Gb SFP+. Karty dostarczyć wraz z wkładkami 10GBASE-LR lub SR. Patchcordy odpowiedniego typu o wymaganej długości. Zastosowanie do połączenia serwera z przełącznikiem w szafie.
* dwie karty dwuportowe FC 16Gb
 |
| Dyski twarde | Możliwość instalacji dysków SATA, SAS, SSD.Zainstalowane dyski:2x 600GB 15k RPM, 3,5“ Hot-Plug lub SSD - skonfigurowane w RAID 1 oraz 10 dysków 8TB 7,2k RPM NLSAS 3,5“ lub SSD - skonfigurowane w RAID 6. |
| Kontroler RAID | Sprzętowy kontroler dyskowy, posiadający min. 4GB nieulotnej pamięci cache, wymagane konfiguracje poziomów RAID: 1, 5, 6, 10, 50, 60. |
| Wbudowane porty | * min. 1 port USB 2.0 oraz 2 porty USB 3.0,
* minimum 1 port video
 |
| Video | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1440x900 |
| Wentylatory | Redundantne |
| Zasilacze | Redundantne, Hot-Plug o mocy co najmniej 700W każdy z dedykowanymi przewodami zasilającymi. Wykonawca powinien dopasować moc zasilaczy do zaproponowanej konfiguracji serwera. |
| Bezpieczeństwo | Płyta wyposażona w moduł TPM. |
| Diagnostyka | Wbudowany panel LCD lub umieszczony na panelu zabezpieczającym lub diody umieszczone na froncie obudowy. |
| Karta Zarządzania | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:* zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
* zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
* szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;
* możliwość podmontowania zdalnych wirtualnych napędów;
* wirtualną konsolę z dostępem do myszy, klawiatury;
* wsparcie dla Ipv6;
* SNMP; IPMI2.0, SSH, Redfish;
* możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;
* możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;
* integracja z Active Directory;
* możliwość obsługi przez dwóch administratorów jednocześnie;
* wsparcie dla dynamic DNS;
* wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
 |
| Certyfikaty | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001
* Serwer musi posiadać deklaracja CE
 |
| Dokumentacja użytkownika | * Dokumentacji w języku polskim lub angi*e*lskim
 |

### Serwer bazodanowy

Wymagane jest dostarczenie 1 szt. serwera spełniającego poniżej opisane minimalne parametry funkcjonalne:

|  |  |
| --- | --- |
| **Cecha** | **Wymagania minimalne** |
| Obudowa | Obudowa Rack o wysokości max 2U z możliwością instalacji do 8 dysków 2.5” Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. |
| Płyta główna | Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
| Chipset | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. |
| Procesor | Zainstalowane dwa procesory ośmiordzeniowe x86 min. 3.3GHz umożliwiające osiągnięcie wyniku min.  130 w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów. |
| RAM | 128GB RDIMM 2666MT/s, na płycie głównej powinny znajdować się minimum 24 sloty przeznaczone do rozbudowy pamięci. Płyta główna powinna obsługiwać do min. 3TB pamięci RAM. |
| Zabezpieczenia pamięci RAM | Memory Rank Sparing, Memory Mirror |
| Gniazda PCI | Min. pięć slotów PCIe Gen 3 w tym dwa sloty PCIe Gen 3 o prędkości min. x16. |
| Interfejsy sieciowe/FC/SAS | Wbudowane dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie SFP+. Karty dostarczyć wraz z wkładkami 10GBASE-LR lub SR. Patchcordy odpowiedniego typu o wymaganej długości. Zastosowanie do połączenia serwera z przełącznikiem w szafie.Dwie karty jednoportowe FC 16Gb HBA. |
| Dyski twarde | Możliwość instalacji dysków SATA, SAS, SSD. Zainstalowane dyski:2x 600GB 10k RPM, Hot-Plug lub SSD - skonfigurowane w RAID 1  |
| Kontroler RAID | Sprzętowy kontroler dyskowy, posiadający min. **2GB** nieulotnej pamięci cache, wymagane konfiguracje poziomów RAID: 1.  |
| Wbudowane porty | * min. 1 port USB 2.0 oraz 2 porty USB 3.0,
* 2 porty video (1 na przednim panelu obudowy, drugi na tylnym)
 |
| Video | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1440 x 900 |
| Wentylatory | Redundantne |
| Zasilacze | Redundantne, Hot-Plug o mocy co najmniej 700W każdy z dedykowanymi przewodami zasilającymi. Wykonawca powinien dopasować moc zasilaczy do zaproponowanej konfiguracji serwera.  |
| Bezpieczeństwo | Płyta wyposażona w moduł TPM. |
| Diagnostyka | Wbudowany panel LCD lub umieszczony na panelu zabezpieczającym lub diody umieszczone na froncie obudowy. |
| Karta Zarządzania | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:* zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
* zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
* szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;
* możliwość podmontowania zdalnych wirtualnych napędów;
* wirtualną konsolę z dostępem do myszy, klawiatury;
* wsparcie dla Ipv6;
* SNMP; IPMI2.0, SSH, Redfish;
* możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;
* możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;
* integracja z Active Directory;
* możliwość obsługi przez dwóch administratorów jednocześnie;
* wsparcie dla dynamic DNS;
* wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
 |
| Certyfikaty | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001
* Serwer musi posiadać deklaracja CE
* Serwer musi posiadać wsparcie dla oferowanego systemu bazodanowego
 |
| Serwerowy system operacyjny | Zamawiający wymaga dostarczenia serwerowego systemu operacyjnego zgodnego z oferowanym oprogramowaniem bazodanowym.  |
| Dokumentacja użytkownika | * Dokumentacji w języku polskim lub angi*e*lskim.
 |

### Serwer bazodanowy zapasowy

Wymagane jest dostarczenie 1 szt. serwera spełniającego poniżej opisane minimalne parametry funkcjonalne:

|  |  |
| --- | --- |
| **Cecha** | **Wymagania minimalne** |
| Obudowa | Obudowa Rack o wysokości max 2U z możliwością instalacji do 8 dysków 2.5” Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. |
| Płyta główna | Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
| Chipset | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |
| Procesor | Zainstalowany jeden procesor ośmiordzeniowy x86 min. 3.3GHz umożliwiający osiągnięcie wyniku min. 130w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org przeprowadzonym w teście dla dwóch procesorów. |
| RAM | 128GB RDIMM 2666MT/s, na płycie głównej powinny znajdować się minimum 24 sloty przeznaczone do rozbudowy pamięci. Płyta główna powinna obsługiwać do min. 3TB pamięci RAM. |
| Zabezpieczenia pamięci RAM | Memory Rank Sparing, Memory Mirror |
| Gniazda PCI | Min. 4 slotów generacji 3  |
| Interfejsy sieciowe/FC/SAS | Wbudowane dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie SFP+. Karty dostarczyć wraz z wkładkami 10GBASE-LR lub SR. Patchcordy odpowiedniego typu o wymaganej długości. Zastosowanie do połączenia serwera z przełącznikiem w szafie.Dwie dodatkowe karty jednoportowe FC 16Gb HBA.  |
| Dyski twarde | Możliwość instalacji dysków SATA, SAS, SSD. Zainstalowane dyski:* 2x 600GB 10k RPM Hot-Plug lub SSD - skonfigurowane w RAID 1
* Możliwość zainstalowania modułu dedykowanego dla hypervisora wirtualizacyjnego, wyposażonego w dwa nośniki typu flash o pojemności min. 64GB z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
 |
| Kontroler RAID | Sprzętowy kontroler dyskowy, posiadający min. **2GB** nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 1.  |
| Wbudowane porty | min. 1 port USB 2.0 oraz 2 porty USB 3.0, 2 porty video (1 na przednim panelu obudowy, drugi na tylnym) |
| Video | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1440 x 900 |
| Wentylatory | Redundantne |
| Zasilacze | Redundantne, Hot-Plug o mocy co najmniej 700W każdy z dedykowanymi przewodami zasilającymi. Wykonawca powinien dopasować moc zasilaczy do zaproponowanej konfiguracji serwera.  |
| Bezpieczeństwo | Płyta wyposażona w moduł TPM. |
| Diagnostyka | Wbudowany panel LCD lub umieszczony na panelu zabezpieczającym lub diody umieszczone na froncie obudowy. |
| Karta Zarządzania | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:* zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
* zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
* szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;
* możliwość podmontowania zdalnych wirtualnych napędów;
* wirtualną konsolę z dostępem do myszy, klawiatury;
* wsparcie dla Ipv6;
* SNMP; IPMI2.0, SSH, Redfish;
* możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;
* możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;
* integracja z Active Directory;
* możliwość obsługi przez dwóch administratorów jednocześnie;
* wsparcie dla dynamic DNS;
* wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
 |
| Certyfikaty | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001Serwer musi posiadać deklaracja CE
* Serwer musi posiadać wsparcie dla oferowanego systemu bazodanowego
 |
| Serwerowy system operacyjny | Zamawiający wymaga dostarczenia serwerowego systemu operacyjnego zgodnego z oferowanym oprogramowaniem bazodanowym.  |
| Dokumentacja użytkownika | * Dokumentacji w języku polskim lub angi*e*lskim
 |

### Macierz główna

Wymagane jest dostarczenie 1 szt. macierzy spełniającej poniżej opisane minimalne parametry funkcjonalne:

|  |  |
| --- | --- |
| **Cecha** | **Wymagania minimalne** |
| Macierz | * Macierz o wysokości min. 2U, posiadająca dwa redundantne kontrolery macierzowe pracujące w trybie active-active wraz z możliwością instalacji min. 24 dysków.
* Macierz musi umożliwiać rozbudowę o moduły: 12 dysków 3,5” o wysokości 2U, 24 dysków 2,5” o wysokości 2U.
* Macierz powinna posiadać dwa kontrolery w jednej obudowie.
 |
| Wymagane dyski | Macierz musi być wyposażona w: 14 dysków 2,5” SSD o pojemności min. 1,8TB każdy, SAS, 12 Gb/s,10 dysków 2,5” o pojemności min. 1,8TB każdy, SAS 12Gb/s, 10k RPM,* Dodatkowy moduł z 12 dyskami 3,5” o pojemności min. 4TB każdy, 12Gb, 7,2k RPM
 |
| Pamięć podręczna (Cache) | min. 32 GB pojemności użytkowej dla danych oraz informacji kontrolnych na każdy kontroler (sumarycznie 64GB).   |
| Interfejsy zewnętrzne | Każdy kontroler musi być wyposażony w 4 porty FC 16Gb, 2 porty 10Gb. Dopuszcza się współdzielenie portów do zarządzania z portami ISCSI.  |
| Dostępność | Odporność na zanik zasilania jednej fazy lub awarię zasilacza macierzy (redundancja układu zasilania). |
| 1) Macierz musi obsługiwać wolumeny:zabezpieczone, które gwarantują odporność na awarię jednocześnie dwóch dysków (RAID 6), zabezpieczone, które gwarantują odporność na awarię jednego dysku (RAID 5), standardowe poziomy RAID 0, 10.2) Macierz dyskowa musi umożliwiać dedykowanie przestrzeni równej pojemności dysku fizycznego jako przestrzeni zapasowej HOT-SPARE lub umożliwiać dedykowanie dowolnego dysku fizycznego jako dysku typu HOT-SPARE.3) Musi istnieć możliwość definiowania dowolnych dysków typu HOT-SPARE.4) Macierz musi umożliwiać konstrukcję urządzenia LUN w taki sposób, aby zawierał dane zabezpieczone różnymi poziomami RAID jednocześnie.5) Macierz musi umożliwiać tworzenie kopii migawkowej w taki sposób, aby dane były zabezpieczone innym poziomem RAID, niż dane źródłowe. |
| Podwójne niezależne przyłącza SAS 12Gb/s do wewnętrznych napędów dyskowych. |
| Odporność na awarię pamięci cache – lustrzany zapis danych oraz technologia zapewniająca ochronę danych z pamięci cache w razie utraty zasilania. |
| Możliwość wykonywania wszystkich napraw, rekonfiguracji, rozbudowy i upgrade’ów (zarówno sprzętu jak i oprogramowania macierzy) w trybie online (bez przerywania pracy systemu). |
| Wspierane systemy operacyjne | Wymagane wsparcie dla różnych systemów operacyjnych, co najmniej Vmware oraz Linux |
| Wymagane wsparcie dla różnych systemów klastrowych, co najmniej Veritas Cluster.  |
| Wsparcie dla mechanizmów dynamicznego przełączania zadań I/O pomiędzy kanałami w przypadku awarii jednego z nich (path failover). Wymagane jest wsparcie dla odpowiednich mechanizmów oferowanych przez producentów systemów operacyjnych: MS Windows, Vmware, Linux. |
| Skalowalność | Wykonywanie rozbudowy sprzętowej w trybie online. |
| Umożliwia rozbudowę do minimum 220 dysków. |
| Możliwość rozbudowy macierzy za pomocą nowych dysków o większych pojemnościach oraz dysków typu SSD/Flash – zoptymalizowanych pod kątem zapisu bądź odczytu. |
| Macierz musi umożliwiać mieszanie dysków o różnych prędkościach obrotowych w ramach jednej półki dyskowej.Macierz musi posiadać możliwość kompresji lub deduplikacji danych. Jeżeli funkcjonalność taka wymaga dodatkowej licencji, to należy je uwzględnić w ofercie. |
| Zarządzanie | Oprogramowanie do zarządzania macierzą przez administratora w ramach pamięci masowej z jednej konsoli administracyjnej. |
| Stałe monitorowanie macierzy przez zdalne centrum serwisowe. |
| Monitorowanie wydajności macierzy według parametrów takich jak: przepustowość oraz liczba operacji I/O  |
| Macierz musi posiadać wbudowaną funkcjonalność typu thin provisioning umożliwiającą alokację wirtualnej przestrzeni dyskowej, do której fizyczne dyski mogą być dostarczone w przyszłości. |
| Możliwość migracji danych w obrębie macierzy | Konieczne jest posiadanie automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane między rożnymi typami dysków w zależności od stopnia obciążenia macierzy dyskowej. Jeżeli wymagana jest dodatkowa licencja na tą funkcjonalność to powinna być zawarta w cenie |
| Macierz musi mieć możliwość migracji wolumenów logicznych LUN pomiędzy różnymi grupami dyskowymi RAID w obrębie macierzy. Migracja musi być wykonywana w trybie on-line. Jeżeli funkcjonalność taka wymaga dodatkowej licencji, to należy je uwzględnić w ofercie.  |
| Lokalna replikacja danych | Możliwość tworzenia kopii danych z poziomu macierzy i wewnątrz macierzy bez angażowania systemu operacyjnego hosta. |
| Możliwość tworzenia i utrzymywania jednocześnie lokalnych kopii danych wewnątrz macierzy dla każdego urządzenia LUN (tzw. kopie point-in-time) przez administratora. |
| Oferowana macierz dyskowa musi umożliwiać wykonanie lokalnej kopii danych na całej zaoferowanej przestrzeni dyskowej. |
| Wymaga jest również funkcjonalność wykonywania kopii wirtualnych typu snapshot.  Jest wymagana licencja na pełną pojemność macierzy oraz maksymalną ilość snapshotów w obrębie macierzy. |
| Kopie migawkowe muszą mieć możliwość prezentacji jako urządzenia LUN w trybie do odczytu i zapisu. Jeżeli ta funkcjonalność wymaga dodatkowej licencji należy ja dostarczyć. |
| Kontrola przepływu danych – QoS | Macierz dyskowa powinna posiadać mechanizmy kontroli wykorzystania zasobów macierzowych na poziomie poszczególnych wolumenów. Kontrola powinna polegać na możliwości dynamicznego ograniczania przepływu danych wyrażanych w MB/s oraz w ilości IOPS poprzez administratora w dowolnym momencie. |
| Współpraca z aplikacjami | Możliwość integracji środowiska Vmware, Veritas InfoScale  |
| Zdalna replikacja danych | Macierz musi posiadać funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie synchronicznym oraz asynchronicznym bez użycia dodatkowych serwerów lub innych urządzeń. Należy dołączyć licencję, jeśli jest wymagana.  |
| Oprogramowanie musi zapewniać funkcjonalność zawieszania i ponownej przyrostowej resynchronizacji kopii z oryginałem. |
| Wymagane do replikacji jest użycie protokołu FC |
| Oferowana macierz dyskowa musi umożliwiać wykonanie w trybie synchronicznym i asynchronicznym zdalnej kopii danych całej powierzchni użytkowej macierzy. |
| Wymiana dysków | Wymiana dysków może być dokonywana przez Zamawiającego |

### Macierz zapasowa

Wymagane jest dostarczenie 1 szt. macierzy spełniającej poniżej opisane minimalne parametry funkcjonalne:

|  |  |
| --- | --- |
| **Cecha** | **Wymagania minimalne** |
| Macierz | * Macierz o wysokości min. 2U, posiadająca dwa redundantne kontrolery macierzowe pracujące w trybie active-active wraz z możliwością instalacji min. 24 dysków. Macierz musi umożliwiać rozbudowę o moduły: 12 dysków 3,5” o wysokości 2U, 24 dysków 2,5” o wysokości 2U.
* Macierz powinna posiadać dwa kontrolery w jednej obudowie
 |
| Wymagane dyski | Macierz musi być wyposażona w: 14 dysków 2,5” SSD o pojemności min. 1,8TB każdy, SAS, 12 Gb/s,10 dysków 2,5” o pojemności min. 1,8TB każdy, SAS 12Gb/s, 10k RPM,* Dodatkowy moduł z 12 dyskami 3,5” o pojemności min. 4TB każdy, 12Gb, 7,2k RPM
 |
| Pamięć podręczna (Cache) | min. 32 GB pojemności użytkowej dla danych oraz informacji kontrolnych na każdy kontroler (sumarycznie 64GB).   |
| Interfejsy zewnętrzne | Każdy kontroler musi być wyposażony w 4 porty FC 16Gb, 2 porty 10Gb**.** Dopuszcza się współdzielenie portów do zarządzania z portami ISCSI. |
| Dostępność | Odporność na zanik zasilania jednej fazy lub awarię zasilacza macierzy (redundancja układu zasilania). |
| 1) Macierz musi obsługiwać wolumeny:zabezpieczone, które gwarantują odporność na awarię jednocześnie dwóch dysków (RAID 6), zabezpieczone, które gwarantują odporność na awarię jednego dysku (RAID 5), standardowe poziomy RAID 0, 10.2) Macierz dyskowa musi umożliwiać dedykowanie przestrzeni równej pojemności dysku fizycznego jako przestrzeni zapasowej HOT-SPARE lub umożliwiać dedykowanie dowolnego dysku fizycznego jako dysku typu HOT-SPARE.3) Musi istnieć możliwość definiowania dowolnych dysków typu HOT-SPARE.4) Macierz musi umożliwiać konstrukcję urządzenia LUN w taki sposób, aby zawierał dane zabezpieczone różnymi poziomami RAID jednocześnie.5) Macierz musi umożliwiać tworzenie kopii migawkowej w taki sposób, aby dane były zabezpieczone innym poziomem RAID,niż dane źródłowe. |
| Podwójne niezależne przyłącza SAS 12Gb/s do wewnętrznych napędów dyskowych. |
| Odporność na awarię pamięci cache – lustrzany zapis danych oraz technologia zapewniająca ochronę danych z pamięci cache w razie utraty zasilania. |
| Możliwość wykonywania wszystkich napraw, rekonfiguracji, rozbudowy i upgrade’ów (zarówno sprzętu jak i oprogramowania macierzy) w trybie online (bez przerywania pracy systemu). |
| Wspierane systemy operacyjne | Wymagane wsparcie dla różnych systemów operacyjnych, co najmniej Vmware oraz Linux |
| Wymagane wsparcie dla różnych systemów klastrowych, co najmniej Veritas Cluster.  |
| Wsparcie dla mechanizmów dynamicznego przełączania zadań I/O pomiędzy kanałami w przypadku awarii jednego z nich (path failover). Wymagane jest wsparcie dla odpowiednich mechanizmów oferowanych przez producentów systemów operacyjnych: MS Windows, Vmware, Linux. |
| Skalowalność | Wykonywanie rozbudowy sprzętowej w trybie online. |
| Umożliwia rozbudowę do minimum 220 dysków. |
| Możliwość rozbudowy macierzy za pomocą nowych dysków o większych pojemnościach oraz dysków typu SSD/Flash – zoptymalizowanych pod kątem zapisu bądź odczytu. |
| Macierz musi umożliwiać mieszanie dysków o różnych prędkościach obrotowych w ramach jednej półki dyskowej.Macierz musi posiadać możliwość kompresji lub deduplikacji danych. Jeżeli funkcjonalność taka wymaga dodatkowej licencji, to należy je uwzględnić w ofercie. |
| Zarządzanie | Oprogramowanie do zarządzania macierzą przez administratora w ramach pamięci masowej z jednej konsoli administracyjnej. |
| Stałe monitorowanie macierzy przez zdalne centrum serwisowe. |
| Monitorowanie wydajności macierzy według parametrów takich jak: przepustowość oraz liczba operacji I/O  |
| Macierz musi posiadać wbudowaną funkcjonalność typu thin provisioning umożliwiającą alokację wirtualnej przestrzeni dyskowej, do której fizyczne dyski mogą być dostarczone w przyszłości. |
| Możliwość migracji danych w obrębie macierzy | Konieczne jest posiadanie automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane między rożnymi typami dysków w zależności od stopnia obciążenia macierzy dyskowej. Jeżeli wymagana jest dodatkowa licencja na tą funkcjonalność to powinna być zawarta w cenie |
| Macierz musi mieć możliwość migracji wolumenów logicznych LUN pomiędzy różnymi grupami dyskowymi RAID w obrębie macierzy. Migracja musi być wykonywana w trybie on-line. Jeżeli funkcjonalność taka wymaga dodatkowej licencji, to należy je uwzględnić w ofercie.  |
| Lokalna replikacja danych | Możliwość tworzenia kopii danych z poziomu macierzy i wewnątrz macierzy bez angażowania systemu operacyjnego hosta. |
| Możliwość tworzenia i utrzymywania jednocześnie lokalnych kopii danych wewnątrz macierzy dla każdego urządzenia LUN (tzw. kopie point-in-time) przez administratora. |
| Oferowana macierz dyskowa musi umożliwiać wykonanie lokalnej kopii danych na całej zaoferowanej przestrzeni dyskowej. |
| Wymaga jest również funkcjonalność wykonywania kopii wirtualnych typu snapshot.  Jest wymagana licencja na pełną pojemność macierzy oraz maksymalną ilość snapshotów w obrębie macierzy. |
| Kopie migawkowe muszą mieć możliwość prezentacji jako urządzenia LUN w trybie do odczytu i zapisu. Jeżeli ta funkcjonalność wymaga dodatkowej licencji należy ja dostarczyć. |
| Kontrola przepływu danych – QoS | Macierz dyskowa powinna posiadać mechanizmy kontroli wykorzystania zasobów macierzowych na poziomie poszczególnych wolumenów. Kontrola powinna polegać na możliwości dynamicznego ograniczania przepływu danych wyrażanych w MB/s oraz w ilości IOPS poprzez administratora w dowolnym momencie. |
| Współpraca z aplikacjami | Możliwość integracji środowiska Vmware, Veritas InfoScale  |
| Zdalna replikacja danych | Macierz musi posiadać funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie synchronicznym oraz asynchronicznym bez użycia dodatkowych serwerów lub innych urządzeń. Należy dołączyć licencję, jeśli jest wymagana.  |
| Oprogramowanie musi zapewniać funkcjonalność zawieszania i ponownej przyrostowej resynchronizacji kopii z oryginałem. |
| Wymagane do replikacji jest użycie protokołu FC |
| Oferowana macierz dyskowa musi umożliwiać wykonanie w trybie synchronicznym i asynchronicznym zdalnej kopii danych całej powierzchni użytkowej macierzy. |
| Wymiana dysków | Wymiana dysków może być dokonywana przez Zamawiającego. |

### Macierz backup/serwer

Wymagane jest dostarczenie 1 szt. macierzy spełniającej poniżej opisane minimalne parametry funkcjonalne:

|  |  |
| --- | --- |
| **Cecha** | **Wymagania minimalne** |
| Obudowa | Obudowa Rack o wysokości max 2U z możliwością instalacji do 12 dysków 3.5” Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. |
| Płyta główna | Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
| Chipset | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |
| Procesor | Zainstalowany jeden procesor ośmiordzeniowy klasy x86, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 80 w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów. |
| RAM | 64GB RDIMM 2666MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 512Gb pamięci RAM. |
| Zabezpieczenia pamięci RAM | Memory Rank Sparing, Memory Mirror  |
| Interfejsy sieciowe/FC/SAS | Wbudowane dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseTDodatkowo zainstalowane karty:* karta dwuportowa 10Gb SFP+ wraz z wkładkami 10GBASE-LR lub SR. Patchcordy odpowiedniego typu o wymaganej długości. Zastosowanie do połączenia serwera z przełącznikiem w szafie.
* -jedna karta dwuportowa FC 16Gb
 |
| Dyski twarde | Możliwość instalacji dysków SATA, SAS, SSD.Zainstalowane dyski:2x 600GB 15k RPM 3,5“ Hot-Plug lub SSD - skonfigurowane w RAID 1 oraz 10 dysków 8TB 7.2k RPM NLSAS 3,5“ lub SSD - skonfigurowane w RAID 6. |
| Kontroler RAID | Sprzętowy kontroler dyskowy, posiadający min. 4GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60, możliwość konfiguracji przestrzeni HOT-SPARE |
| Wbudowane porty | * min. 1 port USB 2.0 oraz 2 porty USB 3.0,
* min. 1 port video
 |
| Video | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1440x900 |
| Wentylatory | Redundantne |
| Zasilacze | Redundantne, Hot-Plug o mocy co najmniej 750W każdy z dedykowanymi przewodami zasilającymi. Wykonawca powinien dopasować moc zasilaczy do zaproponowanej konfiguracji serwera.  |
| Bezpieczeństwo | Płyta wyposażona w moduł TPM. |
| Diagnostyka | Wbudowany panel LCD lub umieszczony na panelu zabezpieczającym lub diody umieszczone na froncie obudowy. |
| Karta Zarządzania | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:* zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
* zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
* szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;
* możliwość podmontowania zdalnych wirtualnych napędów;
* wirtualną konsolę z dostępem do myszy, klawiatury;
* wsparcie dla Ipv6;
* SNMP; IPMI2.0, SSH, Redfish;
* możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;
* możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;
* integracja z Active Directory;
* możliwość obsługi przez dwóch administratorów jednocześnie;
* wsparcie dla dynamic DNS;
* wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
 |
| Certyfikaty | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001Serwer musi posiadać deklaracja CE
* Serwer musi posiadać wsparcie dla oferowanego systemu backupowego
 |
| Dokumentacja użytkownika | * Dokumentacji w języku polskim lub angi*e*lskim.
 |

### Biblioteka LTO

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

|  |  |
| --- | --- |
| **Cecha** | **Wymagania minimalne** |
| Obudowa  | Do zamontowania w szafie rack, maksymalnie 3U dla jednego modułu, wbudowany czytnik kodów kreskowych, redundantne zasilanie wraz z kablami zasilającymi. |
| Napęd | 2 x LTO-7z możliwością instalacji do min. 15 napędów LTO przy wykorzystaniu modułów rozszerzających |
| Interfejs | FC 8Gb/s |
| Liczba slotów | min. 32 w tym minimum pięć slotów we/wy, jeżeli licencjonowana jest liczba slotów – wymagane aktywowanie wszystkich slotówW komplecie min. 1 taśma czyszcząca oraz min. **40 taśm** LTO-7 wraz z etykietami.  |
| Dodatkowe | * interfejs do zarządzania poprzez przeglądarkę WWW oraz możliwość zarządzania bezpośrednio z użyciem wbudowanych klawiszy i wyświetlacza LCD
* wyjmowalne magazynki kieszeni na taśmy w celu łatwego zarządzania większą ilością taśm
* wsparcie dla nośników LTO WORM (Write Once, Read Many), umożliwiających spełnienie norm prawnych dotyczących odpowiednio długiego przechowywania nienaruszonych danych (archiwizacja)
* Obsługa SNMP oraz IP6
* Wsparcie dla technologii szyfrowania backupowanych danych.
 |

### Przełącznik zasobowy do macierzy

Wymagane jest dostarczenie 4 szt. Przełączników w szczególności spełniających poniżej opisane minimalne parametry funkcjonalne:

| **Wymagania minimalne** |
| --- |
| Przełącznik FC musi być wykonany w technologii FC 32 Gb/s i posiadać możliwość pracy portów FC z prędkościami 32, 16, 8 z funkcją autonegocjacji prędkości. |
| Przełącznik FC musi posiadać minimum 24 sloty na moduły FC. Wszystkie wymagane funkcje muszą być dostępne dla 16 portów FC przełącznika.  |
| Przełącznik musi być dostarczony wraz z minimum 14 modułami SFP FC 16 Gb/s oraz dwoma modułami LW min. 8Gb/s. |
| Rodzaj obsługiwanych portów: D\_Port (ClearLink Diagnostic Port), E\_Port, F\_Port, M\_Port (Mirror Port); |
| Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) i szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”. |
| Przełącznik FC musi posiadać nadmiarowe wentylatory N+1  |
| Przełącznik FC musi być wykonany w tzw. architekturze „non-blocking” uniemożliwiającej blokowanie się ruchu wewnątrz przełącznika przy pełnej prędkości pracy wszystkich portów. |
| Urządzenie musi umożliwiać połączenie przełączników w jeden „fabric” (funkcjonalność ISL), dostarczyć licencje, jeśli wymagane. |
| Przełącznik FC musi udostępniać usługę Name Server Zoning – tworzenia stref (zon) w oparciu bazę danych nazw serwerów. |
| Przełącznik FC musi posiadać możliwość wymiany i aktywacji wersji firmware’u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia, bez wymogu ponownego uruchomienia urządzeń w sieci SAN. |
| Przełącznik FC musi posiadać wsparcie dla następujących mechanizmów zwiększających poziom bezpieczeństwa:* Listy Kontroli Dostępu definiujące urządzenia (przełączniki i urządzenia końcowe) uprawnione do pracy w sieci Fabric
* Możliwość uwierzytelnienia (autentykacji) przełączników z listy kontroli dostępu w sieci Fabric za pomocą protokołów DH-CHAP i FCAP
* Możliwość uwierzytelnienia (autentykacji) urządzeń końcowych z listy kontroli dostępu w sieci Fabric za pomocą protokołu DH-CHAP
* Kontrola dostępu administracyjnego definiująca możliwość zarządzania przełącznikiem tylko z określonych urządzeń oraz portów
* Szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2,
* Wskazanie nadrzędnych przełączników odpowiedzialnych za bezpieczeństwo w sieci typu Fabric.
* Konta użytkowników definiowane w środowisku RADIUS lub LDAP
* Szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS
* Obsługa SNMP v3
 |
| Przełącznik FC musi posiadać możliwość konfiguracji przez komendy tekstowe w interfejsie znakowym oraz przez przeglądarkę internetową z interfejsem graficznym.  |
| Przełącznik FC musi mieć możliwość instalacji jednomodowych SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 10km. |
| Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC |
| Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S v1.1 (powinien zawierać agenta SMI-S zgodnego z wersją standardu v1.1) |
| Przełącznik FC musi zapewniać możliwość nadawania adresu IP dla zarządzającego portu Ethernet za pomocą protokołu DHCP |
| Maksymalny dopuszczalny pobór mocy przełącznika FC to 80W |
| Przełącznik FC musi zapewniać możliwość dynamicznego aktywowania portów za pomocą zakupionych kluczy licencyjnych. |
| Przełącznik FC musi zapewniać opóźnienie przy przesyłaniu ramek FC między dowolnymi portami nie większe niż 700ns. |
| Przełącznik FC musi zapewniać sprzętową obsługę zoningu na podstawie portów i adresów WWN |
| Urządzenie musi wspierać mechanizm balansowania ruchem w połączeniach wewnątrz wielodomenowych sieci fabric w oparciu OXID. |
| Możliwość wymiany w trybie „na gorąco”: minimum w odniesieniu do modułów portów Fibre Channel (SFP). |
| Wsparcie dla N\_Port ID Virtualization (NPIV). Obsługa co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika. |
| Szyny do montażu w szafie rack. |

###

### Szafa rack

Wymagane jest dostarczenie 1 szt. szafy spełniającej poniżej opisane minimalne parametry funkcjonalne:

|  |  |
| --- | --- |
| **Cecha** | **Wymagania minimalne** |
| Wysokość wewnętrzna | 42U |
| Szerokość | Szerokość min. 600 mm |
| Głębokość | Głębokość min. 1000 mm |
| Maksymalna nośność | Min. 800 kg |
| Dodatkowe informacje | Drzwi przednie stalowe perforowane z zamkiemDrzwi tylne stalowe perforowane z zamkiemZainstalowane dwa moduły dystrybucji zasilania, min. 16A, 230V, Każdy z modułów wyposażony w gniazda w ilości: C13 - min. 16szt., C19 – min. 2 szt. Ilość gniazd musi zapewnić podłączenie wszystkich dostarczonych elementów (serwery, przełączniki, macierze itd.) z zapewnieniem minimum 4 wolnych gniazd per moduł zasilający. Zamawiający posiada do dyspozycji zasilanie niepodtrzymywane z gniazdem IEC 60309 (1szt.) i zasilanie z podtrzymaniem z gniazdami DATA jednofazowe z uziemieniem (5szt.).Zainstalowane dwa pionowe organizatory kabli |

### Zasilacz awaryjny UPS

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

|  |  |
| --- | --- |
| **Cecha** | **Wymagania minimalne** |
| Technologia | VFI (true on-line, podwójne przetwarzanie energii) |
| Moc znamionowa | 6 kVA / 6 kW |
| Wyjściowy współczynnik mocy (PF) | 1.0 |
| Napięcie wejściowe  | 230 Vac |
| Tolerancja napięcia wejściowego przy obciążeniu mniejszym od 70%; bez przechodzenia na baterie | 110 – 299 Vac |
| Tryb pracy z konwersją częstotliwości | Wymagana praca ze stałą częstotliwością wyjściową 50Hz, przy zasilaniu 60Hz lub odwrotnie. |
| Napięcie wyjściowe  | 230 Vac |
| Częstotliwość wyjściowa | 50/60Hz (programowalna) |
| Wymagania dodatkowe | Automatyczny układ doładowywania baterii i ciągłego sprawdzania stanu naładowania oraz zabezpieczeniechroniące baterie przed głębokim rozładowaniem. |
| Czas podtrzymania | 9 minut dla 100 % obciążenia |
| Baterie | Szczelne, bezobsługowe, w technologii AGM  |
| Szafa baterii | Zamknięty moduł bateryjny |
| Współczynnik szczytu | 3:1 |
| Wymagania | Panel sterujący z wyświetlaczemciekłokrystalicznym LCD oraz sygnalizacją akustyczną |
| Złącze interfejsów | RS232, USB, REPO |
| Wyjściowa listwa do wpięcia UPS do instalacji stałej | Wymagana możliwość podłączenia przewodów o przekroju min 6mm2 |
| Karta sieciowa SNMP | Wymagana |
| Interfejs EPO (do wyłącznika ppoż.) | Wymagane |
| Diagnostyka parametrów urządzeniaUPS i baterii | Automatyczna diagnostyka parametrów urządzenia UPS i baterii na panelu UPS-a i z wykorzystaniem oprogramowania do zarządzania i monitorowania UPS |
| Wymagane | Oprogramowanie zapewniające pełny monitoring, zarządzanie i automatyczny shut-down systemuOperacyjnego. |
| Poziom hałasu w odległości 1m, | < 50 dBAWentylatory o regulowanej prędkości obrotowej w zależności od obciążenia i temperatury |
| Wymagania dodatkowe | Możliwość regulacji z panelu sterującego tolerancji napięcia wejściowego i częstotliwości wejściowej w linii bypassu |
| Certyfikaty i normy | * Spełnienie wszystkich obowiązujących norm w zakresie bezpieczeństwa, kompatybilności elektromagnetycznej potwierdzone deklaracją zgodności CE
 |
| Wymiary zasilacza UPS w szafie rack 19’’ | Maks 2U |
| Wymiary moduł bateryjnego  | Maks. 3 U |
| Zestaw uchwytów do mocowania w szafie rack | Wymagany |
| Dodatkowe  | Instrukcja w języku polskim. |

## Oprogramowanie systemowe i narzędziowe

### Serwerowy system operacyjny

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy:

|  |
| --- |
| **Wymagania minimalne** |
| * Licencja ma mieć charakter wieczysty i nie narażać Zamawiającego na dodatkowe koszty w przyszłym użytkowaniu.
* Licencja obejmująca wszystkie rdzenie procesorów zainstalowanych w zaoferowanych serwerach wirtualnych.
* Zamawiający wymaga licencji grupowej (jeden klucz na wszystkie produkty).
* 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 nielimitowaną liczbę wirtualnych środowisk systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
 |
| Serwerowy system operacyjny (dalej: SSO) posiada następujące, wbudowane cechy: |
| 1 | Posiada możliwość wykorzystania min. 320 logicznych procesorów oraz min. 4 TB pamięci RAM w środowisku fizycznym  |
| 2 | Posiada możliwość wykorzystywania min. 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.  |
| 3 | Posiada możliwość budowania klastrów składających się z min. 64 węzłów, z możliwością uruchamiania do 7000 maszyn wirtualnych.  |
| 4 | Posiada 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 | Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.  |
| 6 | Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.  |
| 7 | Posiada automatyczną weryfikację cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.  |
| 8 | Posiada możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.  |
| 9 | Wbudowane wsparcie instalacji i pracy na wolumenach, które: * pozwalają na zmianę rozmiaru w czasie pracy systemu,
* umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
* umożliwiają kompresję „w locie” dla wybranych plików i/lub folderów,
* umożliwiają zdefiniowanie list kontroli dostępu (ACL).
 |
| 10 | Posiada wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.  |
| 11 | Posiada 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 | Posiada możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET  |
| 13 | Posiada możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.  |
| 14 | Posiada wbudowaną zaporę internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.  |
| 15 | Graficzny interfejs użytkownika.  |
| 16 | Zlokalizowane w języku polskim, następujące elementy: * menu,
* przeglądarka internetowa,
* pomoc,
* komunikaty systemowe.
 |
| 17 | Posiada wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).  |
| 18 | Posiada 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 | Posiada możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: * Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
* 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:
	+ Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
	+ Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
	+ Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
* Zdalna dystrybucja oprogramowania na stacje robocze.
* Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
* Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
* Dystrybucję certyfikatów poprzez http
* Konsolidację CA dla wielu lasów domeny,
* Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.
* Szyfrowanie plików i folderów.
* Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
* Posiada możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów.
* Serwis udostępniania stron WWW.
* Wsparcie dla protokołu IP w wersji 6 (Ipv6),
* Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
* 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 zapewniają wsparcie dla:
* Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
* Obsługi ramek typu jumbo frames dla maszyn wirtualnych,
* Obsługi 4-KB sektorów dysków,
* Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
* Posiada możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model)
* Posiada 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 | Posiada możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.  |
| 24 | Posiada mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.  |
| 25 | Posiada możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.  |

### Licencje dostępowe serwera

W ramach zamówienia Wykonawca zobowiązany jest dostarczyć licencje dostępowe serwera zgodnie
z poniższymi wymaganiami:

|  |  |
| --- | --- |
| **Cecha** | **Wymagania minimalne** |
| Oprogramowanie | MS Windows 2019 Device CAL lub równoważne |
| Inne | Wykonawca zapewni dostęp do spersonalizowanej strony producenta produktów pozwalającej upoważnionym osobom ze strony Zamawiającego na:* Pobieranie zakupionego oprogramowania,
* Pobieranie kluczy aktywacyjnych do zakupionego oprogramowania,
* Sprawdzanie liczby zakupionych licencji w wykazie zakupionych produktów.
 |
| Sposób licencjonowania | * Licencja ma mieć charakter wieczysty i nie narażać Zamawiającego na dodatkowe koszty w przyszłym użytkowaniu.
* Zamawiający wymaga typu licencji MOLP (Microsoft Open License Program) w licencjonowaniu dla jednostek rządowych.
* Licencja ma umożliwiać downgrade do wcześniejszej wersji licencji (2016, 2012) oraz uprawniać do dostępu do zasobów serwera dla określonej liczby urządzeń.
 |
| Kompatybilność | Zamawiający wymaga, aby licencja była kompatybilna z Serwerowym Systemem Operacyjnym SSO opisanym powyżej. |
| Ilość | Serwerowe licencje dostępowe CAL dla dostarczonego oprogramowania do serwerowego systemu operacyjnego dla minimum 500 urządzeń. |

Oprogramowanie Systemowe CAL – opis równoważności:

|  |  |
| --- | --- |
| **Cecha** | **Wymagania minimalne** |
| Sposób licencjonowania | * Licencja ma mieć charakter wieczysty i nie narażać Zamawiającego na dodatkowe koszty w przyszłym użytkowaniu.
* Zamawiający wymaga licencji grupowej (jeden klucz na wszystkie produkty).
* Zamawiający wymaga, aby wszystkie elementy systemu oraz jego licencja pochodziły od tego samego producenta.
* Licencja ma umożliwiać downgrade do poprzednich wersji licencji oraz uprawniać do dostępu do zasobów serwera dla określonej liczby urządzeń.
 |
| Cechy | Licencja powinna zapewnić (w zgodzie z wymaganiami licencyjnymi producenta) możliwość równoległego zarządzania wybranymi usługami przez administratorów serwera, a także dostęp do zasobów serwera dla określonej liczby urządzeń. |
| Kompatybilność | Zamawiający wymaga, aby licencja była kompatybilna z systemem operacyjnym opisanym powyżej. |

### Oprogramowanie bazodanowe

Minimalne wymagania na oprogramowanie systemu zarządzania relacyjną bazą danych:

|  |
| --- |
| **Wymagania minimalne** |
|  | Baza danych ma pracować na fizycznych serwerach. Baza danych musi być zgodna z aplikacją posiadaną przez Zamawiającego. Serwer podstawowy bazodanowy ma działać na posiadanych licencjach ORACLE Zamawiającego, a oprogramowanie bazodanowe ma być wykorzystane na fizycznym serwerze DR. Licencja nie może ograniczać zastosowania wyłącznie do jednej konkretnej aplikacji. Wymagane jest dostarczenie licencji wraz ze wsparciem (dostęp do aktualizacji) na min. 1 rok. |
|  | Baza danych na dedykowanej platformie z przydzieloną odpowiednią ilością licencji dla serwera bazodanowego, zgodną z wymaganiami określonymi w OPZ Możliwość uruchomienia wielu sesji bazy danych przy wykorzystaniu jednego połączenia z serwera aplikacyjnego do serwera bazy danych. Oprogramowanie musi być dostępne na popularne, współczesne platformy sprzętowe i systemowe – 64-bitowe platformy Unix, Linux 32-bit i 64-bit, MS Windows 32-bit i 64-bit. Oprogramowanie nie może mieć limitów na ilość przechowywanych danych – zarówno tekstowych, jak i multimedialnych. |
|  | Dedykowana dla silnika baz danych platforma musi zapewnić jego produkcyjne wykorzystanie w zakresie wszystkich minimalnych parametrów technicznych.  |
|  | Przetwarzanie transakcyjne wg reguł ACID (Atomicity, Consistency, Independency, Durability) z zachowaniem spójności i maksymalnego możliwego stopnia współbieżności. Mechanizm izolowania transakcji powinien pozwalać na spójny odczyt modyfikowanego obszaru danych bez wprowadzania blokad, z kolei spójny odczyt nie powinien blokować możliwości wykonywania zmian. Oznacza to, że modyfikowanie wierszy nie może blokować ich odczytu, z kolei odczyt wierszy nie może ich blokować do celów modyfikacji. Jednocześnie spójność odczytu musi gwarantować uzyskanie rezultatów zapytań odzwierciedlających stan danych z chwili jego rozpoczęcia, niezależnie od modyfikacji przeglądanego zbioru danych.  |
|  | Możliwość zagnieżdżania transakcji – powinna istnieć możliwość uruchomienia niezależnej transakcji wewnątrz transakcji nadrzędnej. Przykładowo – powinien być możliwy następujący scenariusz: każda próba modyfikacji tabeli X powinna w wiarygodny sposób odłożyć ślad w tabeli dziennika operacji, niezależnie czy zmiana tabeli X została zatwierdzona czy wycofana. |
|  | Wsparcie dla wielu ustawień narodowych i wielu zestawów znaków (włącznie z Unicode).  |
|  | Możliwość migracji zestawu znaków bazy danych do Unicode |
|  | Możliwość redefiniowania przez Zamawiającego ustawień narodowych – symboli walut, formatu dat, porządku sortowania znaków za pomocą narzędzi graficznych. |
|  | Skalowanie rozwiązań opartych o architekturę trójwarstwową: możliwość uruchomienia wielu sesji bazy danych przy wykorzystaniu jednego połączenia z serwera aplikacyjnego do serwera bazy danych |
|  | Możliwość otworzenia wielu aktywnych zbiorów rezultatów (zapytań, instrukcji DML) w jednej sesji bazy. |
|  | Wsparcie protokołu XA, Wsparcie standardu JDBC 3.0 |
|  | Zgodność ze standardem ANSI/ISO SQL 2003 lub nowszym.  |
|  | Motor bazy danych powinien umożliwiać wskazywanie optymalizatorowi SQL preferowanych metod optymalizacji na poziomie konfiguracji parametrów pracy serwera bazy danych oraz dla wybranych zapytań. Powinna istnieć możliwość umieszczania wskazówek dla optymalizatora w wybranych instrukcjach SQL. |
|  | Brak formalnych ograniczeń na liczbę tabel i indeksów w bazie danych oraz na ich rozmiar (liczbę wierszy).  |
|  | Wsparcie dla procedur i funkcji składowanych w bazie danych. Język programowania powinien być językiem proceduralnym, blokowym (umożliwiającym deklarowanie zmiennych wewnątrz bloku), oraz wspierającym obsługę wyjątków. W przypadku, gdy wyjątek nie ma zadeklarowanej obsługi wewnątrz bloku, w razie jego wystąpienia wyjątek powinien być automatycznie propagowany do bloku nadrzędnego bądź wywołującej go jednostki programu |
|  | Procedury i funkcje składowane powinny mieć możliwość parametryzowania za pomocą parametrów prostych, jak i parametrów o typach złożonych, definiowanych przez użytkownika. Funkcje powinny mieć możliwość zwracania rezultatów jako zbioru danych, możliwego do wykorzystania jako źródło danych w instrukcjach SQL (czyli występujących we frazie FROM). Ww. jednostki programowe powinny umożliwiać wywoływanie instrukcji SQL (zapytania, instrukcje DML, DDL), umożliwiać jednoczesne otwarcie wielu tzw. kursorów pobierających paczki danych (wiele wierszy za jednym pobraniem) oraz wspierać mechanizmy transakcyjne (np. zatwierdzanie bądź wycofanie transakcji wewnątrz procedury).  |
|  | Możliwość kompilacji procedur składowanych w bazie do postaci kodu binarnego (biblioteki dzielonej) |
|  | Możliwość deklarowania wyzwalaczy (triggerów) na poziomie instrukcji DML (INSERT, UPDATE, DELETE) wykonywanej na tabeli, poziomie każdego wiersza modyfikowanego przez instrukcję DML oraz na poziomie zdarzeń bazy danych (np. próba wykonania instrukcji DDL, start serwera, stop serwera, próba zalogowania użytkownika, wystąpienie specyficznego błędu w serwerze). Ponadto mechanizm wyzwalaczy powinien umożliwiać oprogramowanie obsługi instrukcji DML (INSERT, UPDATE, DELETE) wykonywanych na tzw. niemodyfikowalnych widokach (views). |
|  | W przypadku, gdy w wyzwalaczu na poziomie instrukcji DML wystąpi błąd zgłoszony przez motor bazy danych bądź ustawiony wyjątek w kodzie wyzwalacza, wykonywana instrukcja DML musi być automatycznie wycofana przez serwer bazy danych, zaś stan transakcji po wycofaniu musi odzwierciedlać chwilę przed rozpoczęciem instrukcji, w której wystąpił ww. błąd lub wyjątek |
|  | Możliwość autoryzowania użytkowników bazy danych za pomocą rejestru użytkowników założonego w bazie danych bądź mechanizmu wewnętrznego w stosunku do bazy danych.  |
|  | Baza danych powinna umożliwiać wymuszanie złożoności hasła użytkownika, czasu życia hasła, sprawdzanie historii haseł, blokowania konta przez administratora bądź w przypadku przekroczenia limitu nieudanych logowań. |
|  | Licencja bazy danych powinna być bezterminowa. |
|  | Przywileje użytkowników bazy danych powinny być określane 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). Baza danych powinna umożliwiać nadawanie ww. przywilejów za pośrednictwem mechanizmu grup użytkowników / ról bazodanowych. W danej chwili użytkownik może mieć aktywny dowolny podzbiór nadanych ról bazodanowych. |

### Oprogramowanie systemowe storage

Minimalne wymagania na oprogramowanie systemowe storage:

|  |
| --- |
| **Wymagania minimalne** |
|  | Licencja obejmująca wszystkie rdzenie procesora w zaoferowanym serwerze bazodanowym oraz serwerze bazodanowym DR. |
|  | Oprogramowanie zarządzające podsystemem dyskowym oferujące wysoką dostępności rozwiązania: |
|  | Możliwość tworzenia wolumenów logicznych zapewniając wiele rodzajów ochrony danych takich jak RAID 1, RAID 10, RAID 5  |
|  | Możliwość szyfrowania wolumenów logicznych. |
|  | System musi zapewniać Tiering danych. |
|  | Oprogramowanie musi zapewniać możliwość realizacji kopii migawkowych danych  |
|  | Oprogramowanie musi zapewnić możliwość powiększenia wolumenu danych jak i jego pomniejszania bez przerywania dostępu do danych  |
|  | Oprogramowanie musi oferować obsługę wielu ścieżek dostępu do dysków w relacji host – macierz |
|  | Inteligentne i dynamiczne równoważenie obciążenia pomiędzy wszystkimi dostępnymi ścieżkami |
|  | Dynamiczne równoważenie obciążenia pomiędzy wszystkimi dostępnymi ścieżkami nawet w przypadku uszkodzenia kilku z nich. |
|  | Transparentne zarządzanie operacjami we/wy na ścieżkach, bez wpływu na działające aplikacji. |
|  | Oprogramowanie musi umożliwiać replikację danych aplikacji zachowując ich spójność, realizowaną zarówno na poziomie bloków jak i plików pomiędzy serwerami/hostami. |
|  | Oprogramowania musi zawierać własny system plików dla systemów Linux. |
|  | Oprogramowanie musi oferować klastrowy system plików, który może być jednocześnie używany przez wiele serwerów klastra. |
|  | Oprogramowanie musi oferować duplikację danych.  |
|  | Oprogramowanie musi oferować mechanizmy integracji z platformami baz danych np. Oracle. |
|  | Oprogramowanie musi oferować możliwość utworzenia klastra zapewniającego wysoką dostępność aplikacji bazodanowej |
|  | Oprogramowanie musi oferować narzędzia monitorujące i zarządzające oparte o interfejs graficzny |
|  | Oprogramowanie musi oferować narzędzia zarządzające oparte o wiersz poleceń – CLI |
|  | Licencje musza być bezterminowe oraz objęte 60 miesięcznym wsparciem producenta umożliwiającym dostęp do pomocy technicznej, i do najnowszych wersji oprogramowania w trakcie trwania okresu wsparcia. |

### Oprogramowanie systemowe Load Balancer

Minimalne wymagania na oprogramowanie systemowe Load Balancer:

|  |
| --- |
| **Wymagania minimalne** |
|  | Produkt musi posiadać funkcje równoważenia obciążenia (loadbalace’ing) ruchu TCP/UDP dla usług aplikacyjnych zdefiniowanych na serwerach fizycznych i wirtualnych.Produkt musi być dostarczony z 5 letnim wsparciem producenta. |
|  | Loadbalancer musi zapewniać wydajność na poziomie:* Load Balancing throughput 200 Mbps
* Obsługa jednoczesnych połączeń L4 – 3 000 000
* Wydajność obsługi ruchu TLS (SSL) przez jedną instancje, Ilość nawiązywanych nowych transakcji SSL na sekundę TPS z uwzględnieniem wariantów minimalnej długości klucza szyfrowania.
* SSL TPS (2K Keys): 200
* SSL TPS (1K Keys): 400
 |
|  | Loadbalancer powinien być dostarczony formie programowej „virtual appliance” przystosowany jako szablon do instalacji w środowiskach wirtualizacji dla poniższych platform:* Vmware (OVF)
* vCloud Air (vAPP)
* Microsoft HYPER-V (2008 i 2012)
* Xen
* KVM
* Oracle VirtualBox
 |
|  | Produkt musi umożliwiać terminowanie i akcelerowanie ruchu SSL w celu obsługi aplikacji szyfrowanych oraz odciążenia serwerów rzeczywistych lub virtualnych „SSL offloading” |
|  | Produkt musi zapewniać możliwość przełączania ruchu dla warstwy 7 na podstawie treści „conntent switching” co najmniej w zakresie:* Content Matching: Dopasuj zawartość nagłówka lub treści z zasadą/regułą
* Add Header: Dodaj nagłówek zgodnie z zasadą/regułą
* Del Header: Usuwj nagłówek zgodnie z zasadą/regułą
* Replace Header: Zastępuj nagłówek zgodnie z zasadą/regułą
* Modify URL: Zmieniaj adres URL zgodnie z zasadą/regułą
 |
|  | Produkt musi być wyposażone w zaawansowany system przeźroczystego buforowania „Web Cache” dla protokołów HTTP/HTTPS. |
|  | Produkt musi umożliwiać kompresję treści dla statycznego ruchu HTTP/HTTPS. |
|  | Produkt musi być wyposażone w systemy wykrywania i zapobiegania włamaniom „IPS” dla warstwy 7 z możliwością obsługi reguł VRT SNORT. |
|  | Produkt musi wykorzystywać przynajmniej następujące metody równoważenie ruchu:* Round Robin
* Weighted Round Robin
* Least Connection
* Weighted Least Connection
* Agent-based Adaptive
* SDN Adaptive
* Chained Failover (Fixed Weighting)
* Source-IP Hash
* Layer 7 Content Switching
* AD Group based traffic steering
* Global Server Load Balancing (GSLB)
 |
|  | Produkt musi umożliwiać definiowanie do 256 wirtualnych serwisów VIP i obsługiwać do 1000 serwerów rzeczywistych |
|  | Lodbalancer musi zapewniać wsparcie dla konfiguracji Direct Server Return. |
|  | Produkt musi być wyposażone w wbudowany system wykrywania i obsługi sesji dla Microsoft Terminal Services. |
|  | Produkt musi posiadać wbudowane mechanizmy Session Persistenceco najmniej dla metod:* Source IP (L4)
* SSL SessionID (L4)
* HTTP/HTTPS Browser-session (L7)
* HTTP/HTTPS WebClient-session (L7)
* RDP Login ID (L7)
* Session reconnection for Microsoft RDS
* Port Following for mixed HTTP/HTTPS sessions
 |
|  | Produkt musi umożliwiać konfigurację wsparcia dla S-NAT. |
|  | Produkt musi umożliwiać zarządzania wieloma sieciami wirtualnymi na jednym, wspólnym łączu fizycznym w standardzie 802.1Q. |
|  | Produkt musi wspierać funkcję agregacji portów Link Interface Bonding 802.3ad, link Failover. |
|  | Produkt musi umożliwiać edytowanie i wdrażanie wirtualnych serwisów „w locie”. |
|  |  Akceleracje SSL na urządzeniu powinna umożliwiać wsparcie dla klucza SSL-2048 bit. |
|  |  Musi oferować wsparcie dla certyfikatów z przedłużoną ważnością oraz certyfikaty pośredniczące (*Intermediate certificates*). |
|  | Produkt musi zapewniać wsparcie przynajmniej 200 certyfikatów SSL. |
|  | Produkt musi oferować wsparcie dla protokołu Ipv6 oraz konwersji Ipv4 <-> Ipv6 |
|  | Produkt musi umożliwiać stosowanie certyfikatów firm trzecich. |
|  |  Produkt musi mieć możliwość generowania zapytań CSR w celu potwierdzenia z centrum autoryzacyjnym zgodności certyfikatu. (CSR ***-*** *Certificate Signing Request*) |
|  | Produkt musi umożliwiać sprawdzanie statusów serwerów poprzez internetowy protokół komunikatów kontrolnych.  |
|  | Produkt musi zapewniać metody sprawdzania (próbkowania z poziomu warstwy 7) dostępności usług na serwerach produkcyjnych co najmniej poprzez następujące protokoły: DNS, FTP, HTTP, IMAP, NNTP, POP3, SMTP, WTS(RDP), Telnet. |
|  | Musi w pełni obsługiwać architekturę Microsoft Windows Terminal Services (RDP). |
|  | Loadbalacer musi przeprowadzić auto rekonfiguracje w przypadku wykrycia awarii serwera rzeczywistego.  |
|  | Produkt musi wspierać konfiguracje wysokiej dostępności (Active/Hot Standby) w trybie gwarantowanej ciągłości pracy (Statefull Failover) |
|  | Produkt musi umożliwiać pełną konfiguracje poprzez przeglądarkę internetową. |
|  | Produkt musi zapewniać możliwość bezpiecznego zdalnego logowania dla administratorów poprzez SSH oraz HTTPS.  |
|  | Produkt musi wyświetlać w czasie rzeczywistym informacje o dostępności i wydajności dla:* usług wirtualnych serwisów VIP
* dla serwerów rzeczywistych i wirtualnych
* status funkcjonowania loadbalancera
 |
|  | Produkt musi posiadać zaimplementowany moduł bezpieczeństwa (autoryzacji) w dostępie klientów danej aplikacji do wirtualnych usług serwerowych zdefiniowanych na loadbalancerze. Wymagane wsparcie dla mechanizmów Single Sign On (SSO); Multi-Domain authentication; X.509 client certificate authentication; Two Factor Authentication |
|  | Moduł autoryzacji (Pre-Authentication & SSO) musi integrować się co najminiej z bazami użytkowników zlokalizowanymi: Local Database, ActiveDirectory; Radius; RSA SecurID |
|  | Produkt musi oferować narzędzie do centralnego zarządzania load balancerami, monitorowania wydajności, scentralizowanych i zaplanowanych aktualizacji firmware, tworzenia backup’ów load balancerów. |

### Oprogramowanie wirtualizacyjne

Minimalne wymagania na oprogramowanie do wirtualizacji serwerów:

|  |
| --- |
| **Wymagania minimalne** |
|  | Wykonawca zobowiązany jest do dostarczenia kompletu licencji oprogramowania do wirtualizacji instalowanego na dostarczanych serwerach wirtualizacyjnych, obejmujących łącznie 8 procesorów fizycznych oraz licencji dla potrzeb centralnej konsoli graficznej dla 4 hostów do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności.Licencje powinny być bezterminowe oraz dostarczone z 5 letnim wsparciem |
|  | Warstwa wirtualizacji musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym i nie może być częścią innego systemu operacyjnego. |
|  | Warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 300 MB pamięci operacyjnej RAM serwera fizycznego. |
|  | Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym.  |
|  | Oprogramowanie do wirtualizacji musi zapewnić możliwość przydzielenia maszynom wirtualnym do 128 procesorów wirtualnych. |
|  | Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.  |
|  | Rozwiązanie musi w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.  |
|  | Rozwiązanie musi wspierać następujące systemy operacyjne na maszynie wirtualnej: Windows Server 2008, Windows Server 2012, Windows Server 2012R2, Windows Server 2016, Windows Server 2019, SLES 12, SLES 11, RHEL 7, RHEL 6, RHEL 5. |
|  | Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania środowiskiem serwerów wirtualnych. Konsola graficzna musi być dostępna poprzez przeglądarkę internetową, minimum IE, Firefox, Chrome w najnowszych wersjach. |
|  | Dostęp przez przeglądarkę do konsoli graficznej musi być skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska. |
|  | Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta root. |
|  | Rozwiązanie musi zapewnić możliwość monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej i zdefiniowania alertów informujących o przekroczeniu wartości progowych. |
|  | Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji, bez konieczności instalowania agenta oprogramowania na maszynie wirtualnej. |
|  | Rozwiązanie musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi. |
|  | Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii zapasowych instancji systemów operacyjnych oraz ich odtworzenia w możliwie najkrótszym czasie, bez konieczności instalowania agenta oprogramowania do wykonywania kopii zapasowych.  |
|  | Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością wskazania konieczności zachowania stanu pamięci pracującej maszyny wirtualnej.  |
|  | Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.  |
|  | Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności: Microsoft Active Directory, LDAP.  |
|  | Platforma wirtualizacyjna musi umożliwiać zastosowanie w serwerach fizycznych procesorów o dowolnej ilości rdzeni. |
|  | Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej. |
|  | Rozwiązanie musi umożliwiać wykorzystanie technologii 10GbE w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi.  |
|  | Rozwiązanie musi zapewniać możliwość replikacji maszyn wirtualnych z dowolnej pamięci masowej w tym z dysków wewnętrznych serwerów fizycznych na dowolną pamięć masową w tym samym lub oddalonym ośrodku przetwarzania.  |
|  | Rozwiązanie musi gwarantować współczynnik RPO na poziomie minimum 15 minut  |
|  | Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum.  |
|  | Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek. |
|  | Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek. |
|  | System musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowane wirtualne urządzenia dedykowane dla poszczególnych maszyn wirtualnych. |
|  | Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi, pamięciami masowymi niezależnie od dostępności współdzielonej przestrzeni dyskowej, różnymi wirtualnymi przełącznikami sieciowymi |
|  | Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały automatycznie przełączone na inne serwery infrastruktury. |
|  | Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury.  |
|  | Rozwiązanie musi zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania.  |
|  | 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 lub partycjonowania sieci. |
|  | Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum. Konieczna jest możliwość przenoszenia usług pomiędzy serwerami fizycznymi, wolumenami dyskowymi, klastrami, centrami przetwarzania danych bez przerywania pracy usług. |
|  | Dostarczane licencje muszą umożliwiać rozszerzenie funkcjonalności poprzez upgrade. |

### Oprogramowanie do robienia kopii zapasowych

Minimalne wymagania na oprogramowanie do robienia kopii zapasowych:

|  |
| --- |
| **Wymagania minimalne** |
|  | Oprogramowanie musi umożliwiać łatwą rozbudowę w miarę rozrastania się infrastruktury informatycznej  |
|  | Oprogramowanie musi posiadać scentralizowaną administrację, jedna konsola zarządzająca |
|  | Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej |
|  | System backupowy powinien oferować dla serwerów produkcyjnych backup nie tylko po sieci LAN ale także po sieci SAN. |
|  | System powinien mieć możliwość monitowania i alterowania poprzez email  |
|  | Tworzenie rozwiązania DR dla systemu backupu w sposób w pełni automatyczny z wykorzystaniem tylko i wyłącznie mechanizmów (funkcjonalności) systemu backupowego. Rozwiązanie DR musi umożliwiać replikację obrazów backupowych z wykorzystaniem deduplikacji.  |
|  | Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych. |
|  | Oprogramowanie musi umożliwiać wykonywania skryptów przed i po backupie |
|  | Powinien potrafić wykorzystywać do backupu mechanizm kopii migawkowych systemu Microsoft Windows (VSS) |
|  | Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle.  |
|  | Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory  |
|  | System musi umożliwiać uruchomienie wirtualnej maszyny wprost z kopii zapasowej bez konieczności kopiowania wszystkich danych odtwarzanej maszyny wirtualnej do środowiska produkcyjnego.  |
|  | Oprogramowanie musi wspierać najnowsze wersje systemów do wirtualizacji środowisk: vSphere 6.7, Hyper-V Server 2019  |
|  | Musi być dostępny backup przyrostowy dla serwerów Windows w środowisku Hyper-V |
|  | Dla baz i aplikacji (minimum MS Exchange, MS SQL, Ms SharePoint) oprogramowanie musi wspierać granularne odtwarzanie. |
|  | Rozwiązanie musi w efektywny sposób umożliwiać odtwarzanie kopii zapasowych maszyn fizycznych na maszynie wirtualnej. Funkcjonalność ta musi być dostępna dla systemów operacyjnych Windows i Vmware. |
|  | Należy dostarczyć licencje dla nowo oferowanego środowiska spełniające powyższe funkcjonalności.  |
|  | Oprogramowanie musi posiadać możliwość wykonywania backupów na urządzenia dyskowe, które następnie będą automatycznie powielane na nośniki taśmowe (D2D2T). System backupowy powinien, tak długo jak dane obecne są na dyskach, wykorzystywać je w procesach restore |
|  | System musi umożliwiać równoległe wykonywanie kopii backupu w celu przechowywania na zewnątrz (funkcjonalność mnożenia kopii backupowych musi odbywać się na serwerach systemu backupowego) – z możliwością ustalenia innego poziomu retencji dla kopii.  |
|  | Powinien potrafić backupować i odtwarzać online bazy danych, w szczególności Oracle, SQL Server. Backup-restore bazy Oracle – integracja z narzędziami backupowymi Oracle RMAN.  |
|  | Oprogramowanie musi integrować się z vSphere 6.7 oraz umożliwiać backup/odtwarzanie maszyn wirtualnych z uwzględnieniem spójności zawartości backupowanych maszyn wirtualnych.  |
|  | Backup musi musi być realizowany sprawnie, przyrostowo, pełnie, CBT, exclude vmdk. |
|  | Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. |
|  | Oprogramowanie musi wspierać backup rozciągniętego klastra pomiędzy lokalizacjami. |
|  | Oprogramowanie musi mieć możliwość wykonywania backupów przyrostowych blokowych baz danych Oracle (tylko zmieniających się bloków), bez konieczności skanowania całej bazy danych.  |
|  | System musi posiadać możliwość ustalenia poziomu retencji danych min. (2 tygodnie,1 miesiąc, 1 kwartał, 1 rok). |
|  | Oprogramowanie musi umożliwiać zamykanie kopii typu incremental forever pełnymi kopiami. |
|  | Oprogramowanie musi mieć możliwość rozszerzenia licencji o funkcjonalności kopii do chmury. |
|  | Licencje muszą być bezterminowe oraz objęte 60 miesięcznym wsparciem producenta umożliwiającym dostęp do pomocy technicznej, i do najnowszych wersji oprogramowania w trakcie trwania okresu wsparcia.  |

## Modernizacja sieci LAN w zakresie dostawy i wdrożenia aktywnych urządzeń sieciowych

1. W ramach budowy sieci LAN Wykonawca dostarczy i wdroży aktywne urządzenia sieciowe
o minimalnych parametrach określonych poniżej.
2. Sprzęt musi pochodzić z autoryzowanego przez jego producenta kanału dystrybucji w UE
i nie może być obciążony uprzednio nabytymi prawami podmiotów trzecich (subdystrybucja, niezależni brokerzy) oraz musi być przeznaczony do sprzedaży i serwisu na rynku polskim.
3. Wszystkie urządzenia muszą być fabrycznie nowe wyprodukowane po 1 stycznia 2020r.

### Przełącznik LAN - Przełącznik zarządzający

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

|  |
| --- |
| **Wymagania minimalne** |
| Infrastruktura posiadana przez Zamawiającego:Infrastruktura sieciowa oparta na przełącznikach zarządzalnych HPE, platforma do zarządzania: HPE IMC Standard JG747AAEPrzełączniki powinny być zgodne z posiadaną przez Zamawiającego zintegrowaną platformą do zarządzania HPE IMC oraz z posiadaną infrastrukturą sieciową. |
|  | Co najmniej 24 portów gigabitowych w standardzie 100/1000BaseT  |
|  | Co najmniej 4 porty 10Gb SFP+.  |
|  | Każdy przełącznik wyposażony w 2 wkładki SFP+ 10Gb lub kable DAC niezbędne do podłączenia do infrastruktury |
|  | Przepustowość: minimum 128 Gb/s  |
|  | Wydajność: minimum 90 Mp/s 64byte |
|  | Tablica adresów MAC o wielkości minimum 32000 pozycji |
|  | Obsługa ramek Jumbo |
|  | Minimum 1GB pamięci stałej typu Flash, minimum 1GB pamięci RAM |
|  | Minimum 4MB bufora pakietów |
|  | Dedykowany port do zarządzania poza pasmowego (Ethernet, RJ-45), w pełni niezależny od portów liniowych |
|  | Routing IPv4 – minimum: statyczny, RIPv2, OSPF |
|  | Obsługa protokołu VRRP |
|  | IGMPv1/v2/v3 Snooping; MLDv2, PIM Dense Mode, PIM Sparse Mode |
|  | Obsługa IEEE 802.1s Multiple SpanningTree / MSTP  |
|  | Obsługa 4094 tagów IEEE 802.1Q |
|  | Funkcja Root Guard oraz BPDU protection |
|  | Realizacja łączy agregowanych (LACP)  |
|  | Obsługa list ACL  |
|  | Obsługa standardu 802.1p  |
|  | Funkcja mirroringu portów  |
|  | Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED) |
|  | Funkcja autoryzacji użytkowników zgodna z 802.1x  |
|  | Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+ |
|  | Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az |
|  | Obsługa SNTPv4 lub NTP |
|  | Wsparcie dla funkcji Private VLAN lub równoważnego |
|  | Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Uni-Directional Link Detection (UDLD) |
|  | Wymagane dostarczenie urządzenia wraz z zestawem (uchwyty, szyny itp.) umożliwiającym montaż w szafie 19” |
|  | Wysokość w szafie 19” – 1U |
|  | Dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego przez cały okres gwarancji. Techniczne (niezależnego od zgłaszania usterek) wsparcie telefoniczne w trybie min. 8x5 przez okres co najmniej 5 lat.  |

### Przełącznik LAN - Przełącznik rdzeniowy

Wymagane jest dostarczenie 2 szt. przełączników, o budowie modularnej, spełniających poniżej opisane minimalne parametry funkcjonalne.

*Dopuszcza się również stos (więcej niż 2 szt.) przełączników niemodularnych spełniających wymagania funkcjonalne, wydajnościowe oraz co do ilości i typów portów oraz nadmiarowości wyspecyfikowanych w poniższej tabeli.*

Niezależnie od zaproponowanego rozwiązania wymagana jest konfiguracja zajmująca nie więcej niż 12U w szafie rack. Wymaga się, aby dostarczone przełączniki zostały skonfigurowane w trybie pracy stosu lub klastra. Wykonawca zobowiązany jest do przeniesienia bieżącej konfiguracji z istniejących przełączników Zamawiającego (HP 5406ZL) do dostarczonych przełączników rdzeniowych, w uzgodnieniu z Zamawiającym.

|  |
| --- |
| **Wymagania minimalne** |
| Infrastruktura posiadana przez Zamawiającego:Infrastruktura sieciowa oparta na przełącznikach zarządzalnych HPE, platforma do zarządzania: HPE IMC Standard JG747AAEPrzełączniki powinny być zgodne z posiadaną przez Zamawiającego zintegrowaną platformą do zarządzania HPE IMC oraz z posiadaną infrastrukturą sieciową: |
|  | Typ i liczba portów:  |
| Minimum 16 portów 10Gb SFP+  |
| Minimum 24 porty 1Gb SFP  |
| Minimum 64 porty 100BaseTX/1000BaseT |
|  | Przełącznik musi być wyposażony w kompatybilne z dostarczanymi urządzeniami wkładki SFP i SFP+ i kompatybilne z urządzeniami zamawiającego, w ilości niezbędnej do podłączenia dostarczanej infrastruktury do istniejącej infrastruktury Zamawiającego, z zapewnieniem co najmniej 2 szt. nadmiarowych wkładek w każdym rodzaju. |
|  | Przełącznik musi posiadać moduł zarządzający wyposażony w minimum 1GB pamięci stałej (typu Flash) oraz minimum 4GB pamięci operacyjnej (typu RAM) oraz możliwość instalacji drugiego, redundantnego modułu o takich samych parametrach jak moduł podstawowy |
|  | Redundantne, wewnętrzne zasilacze AC dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia |
|  | Redundantne wentylatory |
|  | Obsługa ramek Jumbo |
|  | Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 2 urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie |
|  | Obsługa sFlow oraz RMON (minimum grupy 1,2,3 i 9) |
|  | Automatyczne wykrywanie przeplotu (AutoMDIX) na portach 100/1000BaseT |
|  | Obsługa 4094 tagów IEEE 802.1Q oraz 4094 jednoczesnych sieci VLAN |
|  | Obsługa standardu IEEE 802.1v protocol VLANs |
|  | Obsługa MAC forwarding table per vlan (możliwość używania takiego samego adresu MAC na różnych portach w różnych VLANach). |
|  | Dostęp do urządzenia przez konsolę szeregową (RS-232 i USB), HTTPS, SSHv2 i SNMPv3 |
|  | Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s) |
|  | Obsługa Secure FTP |
|  | Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP) |
|  | Obsługa dystrybuowanych łączy agregowanych LACP – łączy agregowanych wychodzących z dwóch, różnych, niezależnych i oddzielnie zarządzanych (nie połączonych w stos) przełączników (tzw. Multi-chassis Link Aggregation, MLAG, MC-LAG, Distributed Trunking)  |
|  | Obsługa Simple Network Time Protocol (SNTP) v4 |
|  | Wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping) |
|  | Obsługa protokołów routingu: routing statyczny, RIP v1, RIP v2, OSPF, OSPFv3, VRRP, PIM-SM, PIM-DM |
|  | Obsługa 802.1ad (Q-in-Q) |
|  | Wielkość tablicy routingu: minimum 10000 pozycji IPv4 i minimum 5000 pozycji IPv6 |
|  | Tablica adresów MAC o wielkości minimum 64000 pozycji |
|  | Prędkość matrycy przełączającej nie mniejsza niż 1000 Gb/s |
|  | Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED) |
|  | Automatyczna konfiguracja VLAN dla urządzeń VoIP oparta co najmniej o: RADIUS VLAN (użycie atrybutów RADIUS i mechanizmu LLDP-MED) oraz CDPv2 |
|  | Mechanizmy związane z zapewnieniem jakości usług w sieci: priorytetyzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 8 kolejek sprzętowych, rate-limiting |
|  | Obsługa uwierzytelniania użytkowników zgodna z 802.1x |
|  | Obsługa uwierzytelniania użytkowników w oparciu o lokalną bazę adresów MAC |
|  | Obsługa uwierzytelniania użytkowników w oparciu o adres MAC i serwer RADIUS |
|  | Obsługa uwierzytelniania użytkowników w oparciu o stronę WWW |
|  | Obsługa różnych metod uwierzytelniania (802.1x, MAC, WWW) w tym samym czasie na tym samym porcie |
|  | Obsługa uwierzytelniania wielu użytkowników na tym samym porcie w tym samym czasie |
|  | Obsługa autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+ |
|  | Obsługa autoryzacji komend wydawanych do urządzenia za pomocą serwerów RADIUS albo TACACS+ |
|  | Wbudowany serwer DHCP |
|  | Obsługa funkcji User Datagram Protocol (UDP) helper |
|  | Obsługa blokowania nieautoryzowanych serwerów DHCP |
|  | Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection) |
|  | Obsługa list kontroli dostępu (ACL) bazujących na porcie lub na VLAN z uwzględnieniem adresów IP i portów TCP/UDP bez spadku wydajności urządzenia |
|  | Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Uni-Directional Link Detection (UDLD), Device Link Detection Protocol (DLDP) lub równoważnego |
|  | Obsługa mechanizmu wykrywania usterek kabla dla standardów 100/1000BaseT -Time Domain Reflectometry (TDR) |
|  | Obsługa standardu 802.3az Energy Efficient Ethernet |
|  | Obsługa standardu 802.1AE MACsec |
|  | Obsługa ochrony procesora |
|  | Obudowa umożliwiająca instalację w szafie 19" |
|  | Wymagane dostarczenie urządzenia wraz z zestawem (uchwyty, szyny itp.) umożliwiającym montaż w szafie 19” |
|  | Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji. |
|  | Dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego przez cały okres gwarancji. Techniczne (niezależnego od zgłaszania usterek) wsparcie telefoniczne w trybie min. 8x5 przez okres co najmniej 5 lat.  |

### Przełącznik LAN - Przełącznik dostępowy

Wymagane jest dostarczenie 5 szt. przełączników spełniających poniżej opisane minimalne parametry funkcjonalne:

|  |
| --- |
| **Wymagania minimalne** |
| Infrastruktura posiadana przez Zamawiającego:Infrastruktura sieciowa oparta na przełącznikach zarządzalnych HPE, platforma do zarządzania: HPE IMC Standard JG747AAEPrzełączniki powinny być zgodne z posiadaną przez Zamawiającego zintegrowaną platformą do zarządzania HPE IMC oraz z posiadaną infrastrukturą sieciową: |
|  | Typ i liczba portów:  |
| Minimum 20 portów 1G/10GbE SFP+  |
| Przełącznik musi być wyposażony w kompatybilne z dostarczanymi urządzeniami wkładki SFP+ w ilości niezbędnej do podłączenia do przełączników rdzeniowych, przewodów do utworzenia stosów oraz 10 wkładek SFP+ (na przełącznik) kompatybilnych z wkładkami zamontowanymi w serwerach |
|  Minimum 2 porty 40GbE QSFP+ lub co najmniej 2 dedykowane porty umożliwiające łączenie w stos. Wydajność portów stackujących co najmniej 40 Gbps na port. Oprogramowanie przełącznika musi umożliwiać połączenie co najmniej 4 urządzeń w stos. Przełączniki połączone w stos z punktu widzenia reszty infrastruktury muszą być widoczne jako jedno urządzenie, czyli muszą tworzyć jedno logiczne urządzenie zarządzane z jednej linii komend. |
|  Cztery przełączniki muszą być skonfigurowane w dwa stosy pod dwa przełączniki. Piąty będzie pracował samodzielnie. |
|  | Wbudowany, dodatkowy, dedykowany port Ethernet do zarządzania poza pasmem - out of band management |
|  | Port konsoli RS232 ze złączem DB9 lub RJ45 |
|  | Przepustowość minimum 480 Gb/s  |
|  | Wydajność: minimum 285 Mp/s  |
|  | Przełączanie w warstwie 2 i 3 modelu OSI |
|  | Wielkość bufora pakietów (packet buffer): minimum 9MB  |
|  | Minimum 256MB pamięci typu Flash |
|  | Minimum 2GB pamięci operacyjnej |
|  | Przełącznik wyposażony w redundantne, modularne wentylatory (minimum dwa niezależne moduły wentylatorów) |
|  | Dwa wbudowane (wewnętrzne, modularne) zasilacze AC dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia.  |
|  | Funkcja łączenia w stos grupy przełączników, urządzenia połączone w stos widziane jako jedno logiczne urządzenie ze wspólnym zarządzaniem. Wymagane jest by urządzania tworzące stos mogły posiadać łącznie nie mniej niż 360 portów 10GbE SFP+.  |
|  | Realizacja łączy agregowanych w ramach różnych przełączników będących w stosie  |
|  | Tablica adresów MAC o wielkości minimum 64000 pozycji |
|  | Obsługa ramek Jumbo  |
|  | Obsługa Quality of Service |
|  | Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol |
|  | Obsługa sieci IEEE 802.1Q VLAN – 4094 sieci VLAN oraz IEEE 802.1ad QinQ |
|  | Obsługa IGMP Snooping v1/v2/v3, PIM Snooping, MLD snooping v1/v2 oraz IPv6 PIM Snooping |
|  | Routing IPv4 – statyczny i dynamiczny (min. RIP, IS-IS, OSPF) |
|  | Routing IPv6 – statyczny i dynamiczny (min. RIPng, IS-ISv6, OSPFv3) |
|  | Obsługa ECMP (Equal Cost Multi Path)  |
|  | Tablica routingu o pojemności co najmniej 1000 wpisów  |
|  | Serwer DHCP, obsługa opcji 82 (snooping i relay), DHCP snooping |
|  | Obsługa standardu 802.1p |
|  | Możliwość zmiany wartości pola DSCP i/lub wartości priorytetu 802.1p |
|  | Możliwość centralnego uwierzytelniania administratorów na serwerze RADIUS |
|  | Zarządzanie poprzez port konsoli, SNMP v.1, 2c i 3, Telnet, SSH v.2 |
|  | Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) oraz LLDP-MED |
|  | Obsługa sFlow lub Netflow |
|  | Obsługa Network Time Protocol (NTP), Simple Network Time Protocol (SNTP)  |
|  | Wysokość w szafie 19” – 1U  |
|  |  Wymagane dostarczenie urządzenia wraz z zestawem (uchwyty, szyny itp.) umożliwiającym montaż w szafie Rack 19” |
|  | Dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego przez cały okres gwarancji. Techniczne (niezależnego od zgłaszania usterek) wsparcie telefoniczne w trybie min. 8x5 przez okres co najmniej 5 lat.  |

## Dostawa i wdrożenie Szpitalnego Systemu Informatycznego SSI

### Wymogi dotyczące interoperacyjności lub migracji dla oferowanego SSI

1. Wykonawca zobowiązuje się dostarczyć Zamawiającemu wymagane funkcjonalności SSI, poprzez zmodernizowanie i rozbudowanie istniejącego systemu w taki sposób, aby w jak najszerszym zakresie zostały zaspokojone potrzeby Zamawiającego. Zamawiający dopuszcza wymianę posiadanego rozwiązania. Koniecznym jest zachowanie pełnej wzajemnej interoperacyjności nowo wdrażanych modułów/grup funkcjonalności, a także w przypadku rozbudowy, pełnej interoperacyjności z modułami/grupami/systemami funkcjonalności funkcjonującymi u Zamawiającego.
2. W przypadku wymiany SSI na inny niż obecnie wykorzystywany, Wykonawca zobowiązany jest do zachowania poziomu interoperacyjności z systemem ERP działającym w części „szarej” szpitala w zakresie nie mniejszym niż obecnie co wskazano w rozdziale II.4.4 pkt.20.
3. Zamawiający dopuszcza wymianę wyłącznie w przypadku, gdy zaproponowane rozwiązanie zapewni wszystkie funkcjonalności działające obecnie w środowisku Zamawiającego gwarantując że użytkownicy nie będą musieli pracować równolegle w dwóch szpitalnych systemach informatycznych.
4. W przypadku wymiany HIS, Wykonawca musi zapewnić licencje umożliwiające pracę w systemie nielimitowanej ilości użytkowników dla działających obecnie u Zamawiającego funkcjonalności HIS. Alternatywne rozwiązanie musi działać z wykorzystaniem posiadanych licencji na bazę danych lub Wykonawca musi je dostarczyć na własny koszt.
5. Zintegrowany System Informatyczny, stanowiący źródło Elektronicznej Dokumentacji Medycznej EDM musi mieć zaimplementowane i uruchomione mechanizmy integracji oraz zapewnić prawidłową integrację z systemem EDM.
6. W SSI należy zapewnić spełnienie przez ten system wymagań Web Content Accessibility Guidelines (WCAG 2.0), z uwzględnieniem poziomu AA, określonych w załączniku nr 4 do rozporządzenia.

### Dostępność dostarczanego rozwiązania

Zintegrowany System Informatyczny SSI działa w trybie 24 godzinnym przez wszystkie dni w roku z dostępnością co najmniej na poziomie 99% w skali miesiąca. 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). Planowane prace (tzw. down time) odbywają się w godzinach od 03:30 do 06:30. W ciągu jednego miesiąca mogą odbyć się maksymalnie cztery takie przerwy. Czas planowych prac (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).

### Wymagany stan docelowy

Zamawiający oczekuje dostarczenia Szpitalnego Systemu Informatycznego co najmniej z modułami:

Zakres dostawy i wdrożenia oprogramowania:

|  |
| --- |
| **Dostawa i wdrożenie Oprogramowania Aplikacyjnego** |
| **l.p.** | **Zakres** | **Typ licencji**  | **Ilość** |
| 1. | Elektroniczna Dokumentacja Medyczna | bezterminowa | Licencja otwarta\* |
| 2. | Rejestracja On-line | bezterminowa | Licencja otwarta\* |
| 3. |  HIS – Zakażenia Szpitalne | bezterminowa | Licencja otwarta\* |
| 4. |  LIS – integracja HIS-LIS | bezterminowa | 1 |

*\* Licencje/sublicencje bez ograniczeń ilości jednocześnie aktywnych użytkowników*

Oferowane produkty w ramach SSI muszą posiadać i realizować co najmniej funkcjonalności przedstawione w rozdziale II.4 SOPZ.

Szpitalny System Informatyczny aktualnie posiadany i eksploatowany przez Zamawiającego:

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Wyszczególnienie** | **Integracja dostarczanego oprogramowania** |
| 1. | 1. System informatyczny AMMS/Infomedica firmy Asseco Poland S.A.Moduły zintegrowanego systemu informatycznego: * Moduł: AMMS - Pulpity
* Moduł: AMMS - Oddział
* Moduł: AMMS - Apteczka
* Moduł: AMMS - Apteka
* Moduł: AMMS - Rejestracja
* Moduł: AMMS - Pracownia
* Moduł: AMMS - Rehabilitacja
* Moduł: AMMS - Gabinet
* Moduł: AMMS - Izba Przyjęć
* Moduł: AMMS - Blok Operacyjny
* Moduł: AMMS - Punkt Pobrań
* Moduł: AMMS - Rozliczenia
* Moduł: AMMS – Statystyka
* Moduł: Wymiana danych
* Moduł: Szpitalny Portal Informacyjny

2. . Baza danych zintegrowanego systemu informatycznego:- 2xCPU Oracle 11g Standard Edition One. | TAK |
| 2. | RIS firmy TMS Soft | TAK |
| 3. | PACS firmy AGFA | TAK |
| 4. | LIS firmy Marcel (Mikrobiologia, Serologia, Bank Krwi) | TAK |
| 5 | LIS firmy Filab (analityka) | TAK |

### Oprogramowanie aplikacyjne – wymagania ogólne

1. Wykonawca zobowiązuje się dostarczyć Zamawiającemu określone funkcjonalności SSI, poprzez dostawę nowego rozwiązania w taki sposób, aby w jak najszerszym zakresie zostały zaspokojone potrzeby Zamawiającego. W chwili obecnej Zamawiający korzysta z oprogramowania SSI dla części „białej” oraz „szarej” Infomedica/AMMS produkcji Asseco Poland.
2. W przypadku rozbudowy SSI Zamawiającego w zakresie dostarczonego rozwiązania informatycznego w postaci oprogramowania aplikacyjnego, budującego usługi elektroniczne Zamawiający wymaga, aby w pełni współpracowało ono z posiadanym i eksploatowanym przez Zamawiającego SSI bez konieczności dokonywania zmian w SSI.
3. Zakres danych znajdujących się w HIS obejmujących dokumentowanie z procesu udzielania świadczeń składających się na dokumentacje zbiorczą i indywidualną zarówno zewnętrzną jak i wewnętrzną powinien być zgodny z zakresem określonym przepisami prawa, płatnika publicznego świadczeń, akredytacji i przekazanych przez szpital wzorów dokumentów.
4. Zasilenie początkowe danymi słownikowymi takimi jak:
	1. Słownik ICD 9 i ICD 10,
	2. Słownik Instytucji właściwych UE,
	3. Miejscowości i kody terytorialne,
	4. Inne które zostaną ustalone z Zamawiającym w ramach analizy przedwdrożeniowej.
5. Dane jakie powinny być dostępne z oprogramowania objętego przedmiotem zamówienia powinny obejmować minimum:
	1. dane o pacjentach i ich opiekunach,
	2. słownik lekarzy (pracujących i kierujących) wraz z nr prawa wykonywania zawodu oraz specjalizacjami,
	3. słownik instytucji kierujących,
	4. dane o płatnikach i umowach,
	5. dane statystyczne rozliczonych pacjentów do NFZ (z roku rozliczeniowego w którym zostanie uruchomiony system),
	6. kolejki oczekujących,
	7. słownik kontrahentów/dostawców,
	8. słownik jednostek wraz z kodami resortowymi, ilością łóżek,
	9. słownik użytkowników.
6. System powinien umożliwić wygenerowanie prawidłowych (zgodnych z opublikowanymi przez NFZ plikami walidującymi) komunikatów wymiany danych z NFZ dotyczących wszystkich umów na świadczenia w bieżącym roku rozliczeniowym i roku następnym, powinien umożliwić ciągłość rozliczeń z NFZ począwszy od dnia uruchomienia SSI na środowisku produkcyjnym w tym również rozliczenie z NFZ dla pobytów otwartych na dzień uruchomienia SSI na środowisku produkcyjnym.
7. W Systemie muszą być zaimplementowane mechanizmy walidacji haseł zgodnie z wymaganiami ustawowymi przewidzianymi dla rodzaju danych przetwarzanych przez System.
8. System musi być dostosowany do struktury organizacyjnej Zamawiającego.
9. System musi tworzyć i utrzymywać log systemowy (datę i godzinę z dokładnością do sekundy; adres IP stacji lub jej nazwa, unikalny identyfikator użytkownika; jeżeli dane w Systemie uległy zmianie to również informacje o tym, z jakiej wartości i na jaką wartość została dokonana zmiana), rejestrujący w szczególności zapisy o zalogowaniu do Systemu i wylogowaniu z Systemu każdego z użytkowników.
10. System musi mieć możliwość utrzymania następujących przedmiotowych zbiorów słownikowych przez administratora:
	* płatników (w tym oddziałów NFZ) i umów z nimi zawartych,
	* jednostek i lekarzy kierujących,
	* katalogów badań,
	* katalogu leków, w tym receptariusza szpitalnego,
	* cenników.
11. System musi mieć możliwość definiowania listy personelu białego (w szczególności lekarzy, pielęgniarek, położnych, techników) i ich specjalności zgodnie ze słownikiem i wymaganiami NFZ.
12. System musi być zintegrowany, przez co rozumie się zintegrowaną pracę wszystkich systemów/modułów w oparciu o swobodną, automatyczną wymienialność danych pomiędzy elementami (modułami) systemu.
13. System musi pozwalać na obsługę zdarzeń niepożądanych zgodnie z nadanymi w systemie uprawnieniami.
14. System musi posiadać możliwość zarejestrowania oraz analizy zdarzeń niepożądanych zgodnie ze standardami akredytacyjnymi publikowanymi przez Centrum Monitorowania Jakości w Ochronie Zdrowia.
15. Dostarczane rozwiązanie musi być przystosowane do wymiany danych z platformami ogólnokrajowymi P1/P2. Dane zaimportowane do SSI z aktualnie użytkowanego oprogramowania muszą być spójne z nowo wprowadzanymi, edytowalne, podlegające analizie i spełniające warunki walidacji dla określonych typów pól.
16. Zamawiający zapewni współpracę z Producentem SSI wskazanego w pkt II.4.3 przy uzyskaniu przez Wykonawcę opisów interfejsów do integracji, natomiast wykonanie integracji jest obowiązkiem Wykonawcy. Ustalenie kosztów integracji z systemami posiadanymi przez Zamawiającego jest obowiązkiem Wykonawcy. Zamawiający nie odpowiada za zawartość merytoryczną dokumentacji w zakresie opisów interfejsów, którą przekaże zainteresowanym stronom producent SSI.
17. Zamawiający dopuszcza integrację z obecnymi systemami dziedzinowymi tylko i wyłącznie poprzez wyspecyfikowane interfejsy, których implementację udostępnia dany system dziedzinowy ze względu na to, że integracja bezpośrednia na poziomie bazy danych mogłaby doprowadzić do niekontrolowanej utraty integralności danych co w skrajnym przypadku grozi uszkodzeniem danych wrażliwych procesu leczenia pacjentów.
18. Zamawiający nie przewiduje pośredniczenia w rozmowach z firmami trzecimi dotyczących integracji z ich systemami. Zamawiający wyjaśnia, że koszty integracji są częścią kosztu oferty składanej przez Wykonawcę w niniejszym postępowaniu. W związku z powyższym załącza do SIWZ posiadaną dokumentację wymiany danych tj. Opis komunikatów stanowiących załącznik nr 1A do SIWZ.
19. Zamawiający wymaga spełnienia następujących warunków przez wdrożone oprogramowanie aplikacyjne:
	1. zachowanie ciągłości obecnie stosowanych przez Zamawiającego oznaczeń dokumentacji medycznej,
	2. umożliwienie kontynuacji sprawozdawania i rozliczania świadczeń udzielonych pacjentom przebywającym w szpitalu od kilkunastu lat (możliwość przesłania do NFZ pełnej historii hospitalizacji oraz historii rozliczeń), przy wykorzystaniu jednego modułu/oprogramowania,
	3. umożliwienie dokonywania korekt zakwestionowanych przez NFZ świadczeń sprawozdanych i rozliczonych od roku 2010,
	4. zachowanie przekazanej do NFZ historycznej numeracji zestawów świadczeń i procedur rozliczeniowych oraz zachowanie historycznej numeracji wszystkich innych danych przekazanych do NFZ i potwierdzonych, takich jak id uprawnień, numeracja sesji, numer przepustki, itp.,
	5. zapewnienie możliwości wykonywania archiwalnych statystyk i raportów,
	6. zapewnienie możliwości wykonywania kopii zapasowych struktur danych w trakcie ich pracy,
	7. posiadanie sprawnego mechanizmu archiwizacji danych i mechanizmów gwarantujących spójność danych. Wymagane jest wzajemne współdziałanie modułów systemu medycznego i portalowego poprzez powiązania logiczne i korzystanie ze wspólnych danych przechowywanych na serwerach,
	8. zapewnienie współpracy w zakresie eksportu danych z innym oprogramowaniem - pakietem oprogramowania biurowego (arkusz kalkulacyjny, edytor tekstów),
	9. komunikaty systemowe i komunikacja z użytkownikiem w języku polskim,
	10. możliwość korzystania z rozbudowanych podpowiedzi.
20. Zakres wymiany danych pomiędzy systemem HIS i ERP wykorzystywany obecnie u Zamawiającego:
21. Dane udostępniane przez system ERP:
* Dane na potrzeby windykacji dotyczącej pacjentów.
* Koszty wykonywanych świadczeń.
* Dane do wyliczenia kosztów osobodnia personelu.
1. Dane udostępniane przez system HIS:
* Dokumenty kasowe.
* Faktury sprzedaży.
* Statystyka wykonań procedur ze wskazaniem jednostek zlecających.
* Liczba osobodni, liczba pobytów, liczba łóżek, średnie obłożenie łóżek, liczba hospitalizacji (zakres przekazywanych danych może być definiowany).
* Dokumenty księgowe: PW, PZ.
* Indeksy leków oraz ceny tych leków.
* Rozchody leków na OPK.
1. Słowniki wspólne:
* Słownik kontrahentów.
* Słownik ośrodków powstawania kosztów.
* Słownik placówek kosztowych.
* Słownik rodzajów kosztów.
* Słownik sposobów płatności wykorzystywanych w dokumentach sprzedaży / zakupu.

|  |  |
| --- | --- |
| **L.p.** | **Zakres integracji** |
|  | Wymagania dla dwukierunkowej integracji z Systemem ERP  |
|  | System powinien umożliwiać wymianę danych o ilości zleceń wewnętrznych- ilości wykonanych badań laboratoryjnych z systemu LIS/HIS - ilości wykonanych badań diagnostycznych z systemu HIS |
|  | System powinien umożliwiać wymianę danych statystycznych, co najmniej w zakresie:* Ilość pacjentów wypisanych/leczonych
* Ilość wykonanych procedur
* Liczba łóżek
* Ilość wykonanych porad
 |
|  | System powinien umożliwiać wymianę danych o przychodach z Apteki, co najmniej w zakresie:* dane wartościowe dotyczące przychodów leków na poszczególne magazyny
* dane o rozrachunkach wynikających z tych przychodów
 |
|  | System powinien umożliwiać wymianę danych o rozchodach z Apteki, co najmniej w zakresie:* dane wartościowe dotyczące rozchodów materiałów na poszczególne OPK w podziale na koszty szczegółowe
 |
|  | System powinien umożliwiać wymianę danych o lekach wraz z cenami, co najmniej w zakresie:* indeks materiałowy (nazwa leku, indeks, średnia cena, jednostka miary,
 |
|  | System powinien umożliwiać wymianę danych w zakresie obsługi faktur:* zapis danych o wystawionych dokumentach sprzedaży w systemie HIS wraz z rozrachunkami, dla nowo wystawianych faktur
 |
|  | System powinien umożliwiać przekazywanie danych kosztowych w zakresie:* koszty osobodni w podziale na OPK
* wartość wycenionych na dany miesiąc świadczeniach medycznych
 |
|  | System powinien umożliwiać wymianę danych o rozchodach z Apteczki Oddziałowej, co najmniej w zakresie:* Wartość podanych pacjentom leków z podziałem na Ośrodki Powstawania Kosztów
 |

1. Wdrażanie dostarczanego oprogramowania aplikacyjnego musi uwzględniać ciągłość funkcjonowania Zamawiającego i eksploatacji posiadanego przez niego SSI. Przez sformułowanie ciągłość pracy Zamawiający rozumie takie przeprowadzenie wdrożenia i migracji danych (na nowe środowisko), które nie będzie powodowało przerw w pracy poszczególnych jednostek organizacyjnych Zamawiającego. W szczególności zapewniona będzie ciągłość: rejestrowania i korzystania z danych przez personel Zamawiającego, dokonywania rozliczeń z NFZ i kontrahentami, sporządzania wymaganej prawem sprawozdawczości. Wszelkie przerwy w tym zakresie wynikające z prowadzonych przez Wykonawcę prac wdrożeniowych muszą zostać uzgodnione z producentem SSI i zatwierdzone przez Zamawiającego.

### Szpitalny System Informatyczny – wymagania szczegółowe

Dostawa i wdrożenie SSI obejmuje dostawę odpowiednich licencji oprogramowania dla Szpitalnego Systemu Informatycznego, o funkcjonalnościach i na warunkach nie mniejszych niż opisane poniżej:

#### HIS – zakażenia szpitalne:

|  |  |
| --- | --- |
| L.p. | **Wymagania ogólne** **Parametry wymagane** |
|  | Moduł realizuje wspomaganie Zakładu Opieki Zdrowotnej w zakresie kontroli występowania zakażeń szpitalnych i zapobiegania tym zakażeniom, zgodnie z odpowiednimi przepisami prawa. W szczególności: |
|  | prowadzenie Rejestru Kart Rejestracji Zakażenia Szpitalnego |
|  | wydruki na podstawie danych Rejestru Kart Rejestracji Zakażenia Szpitalnego |
|  | prowadzenie Rejestru Kart Rejestracji Drobnoustroju Alarmowego |
|  | wydruki na podstawie danych Rejestru Kart Rejestracji Drobnoustroju Alarmowego |
|  | System musi umożliwiać dodanie czynnika alarmowego do karty IKRD/CzA na podstawie wyniku badania mikrobiologicznego |
|  | prowadzenie Rejestru zgłoszeń zachorowania na chorobę zakaźną |
|  | wydruki na podstawie danych Rejestru zgłoszeń zachorowania na chorobę zakaźną |
|  | prowadzenie Rejestru zgłoszeń zachorowania (podejrzenia zachorowania) na AIDS lub zgłoszenia zakażenia (podejrzenia zakażenia) HIV |
|  | wydruki na podstawie danych Rejestru zgłoszeń zachorowania (podejrzenia zachorowania) na AIDS lub zgłoszenia zakażenia (podejrzenia zakażenia) HIV |
|  | prowadzenie Rejestru zgłoszeń zachorowania (podejrzenia zachorowania) na chorobę przenoszoną drogą płciową |
|  | wydruki na podstawie danych Rejestru zgłoszeń zachorowania (podejrzenia zachorowania) na chorobę przenoszoną drogą płciową |
|  | prowadzenie Rejestru zgłoszeń zachorowania (podejrzenia zachorowania) na gruźlicę |
|  | wydruki na podstawie danych Rejestru zgłoszeń zachorowania (podejrzenia zachorowania) na gruźlicę |
|  | prowadzenie Rejestru zgłoszeń zgonu (podejrzenia zgonu) z powodu choroby zakaźnej |
|  | wydruki na podstawie danych Rejestru zgłoszeń zgonu (podejrzenia zgonu) z powodu choroby zakaźnej |
|  | System musi informować o wcześniejszym zgłoszeniu pacjenta w ramach danego formularza zgłoszenia zachorowania, w ramach danego pobytu |
|  | prowadzenie Rejestru obserwacji potencjalnych źródeł zakażenia (wkłucia obwodowe, wkłucia centralne, cewniki, respiratory, operacje, infekcje) |
|  | System musi umożliwiać zbiorczy wydruk kart pomocniczych i formularzy zgłoszenia zachorowania. |
|  | prowadzenie Rejestru podejrzeń ognisk epidemicznych |
|  | wydruki na podstawie danych Rejestru podejrzeń ognisk epidemicznych |
|  | prowadzenie Rejestru potwierdzonych ognisk epidemicznych |
|  | wydruki na podstawie danych Rejestru potwierdzonych ognisk epidemicznych |
|  | raporty zgodne z odpowiednim Rozporządzeniem Ministra Zdrowia, |
|  | analizy ilościowe zakażeń szpitalnych, |
|  | Współpraca z systemem RCH oraz Laboratorium w zakresie podań antybiotyków i zleceń badań do pracowni mikrobiologicznej: |
|  |  - monitorowanie o konieczność założenia Indywidualnej Karty Zakażeń Szpitalnych w przypadku podania antybiotyku powyżej 3 dni |
|  |  - monitorowanie o konieczność założenia Indywidualnej Karty Zakażeń Szpitalnych w przypadku wystąpienia patogenu w badaniu mikrobiologicznym |
|  | System współpracuje z modułem Ruch Chorych w zakresie powiadomienia o konieczności założenia Indywidualnej Karty Zakażenia Szpitalnego, w przypadku wystąpienia temperatury ciała pacjenta powyżej X godz. od przyjęcia do szpitala. |
|  | System umożliwia podgląd pacjentów gorączkujących powyżej określonej w parametrze wysokości temperatury  |
|  | Prowadzenie Rejestru Kart zakażeń dla pracowników  |
|  | Prowadzenie Rejestru szczepień i odmów szczepień pracowników  |
|  | Możliwość dostosowania wydruku Kart zakażeń |
|  | Możliwość dostosowania widoczności pól na Kartach zakażeń oraz na Kartach drobnoustroju |
|  | Możliwość definicji walidacji pól na Kartach zakażenia oraz Kart drobnoustroju |
|  | Możliwość definicji powiązań zgłoszeń zachorowań na choroby zakaźne z: -patogenem -rozpoznaniem  |
|  | Możliwość definicji diagnoz pielęgniarskich pod kątem wymagalności zakładania Kart zakażeń  |
|  | Możliwość definicji rozpoznań dla których zakładana jest Karta zakażenia  |
|  | Możliwość definicji zakładania Kart zakażeń na podstawie założonych Kart drobnoustroju  |
|  | Zależność Kart zakażeń na podstawie założonych Kart drobnoustroju |
|  |  - szybki podgląd listy pacjentów dla nowo założonych: kart obserwacji, kart zakażenia, kart drobnoustroju, alert-patogenów  |

#### Rejestracja On-line (Portal Pacjenta)

|  |  |
| --- | --- |
|  | **Wymagania ogólne** **Parametry wymagane** |
| 1. 1.
 | System zapewnia przesyłanie danych z wykorzystaniem bezpiecznego kanału komunikacji - umożliwia szyfrowanie transmisji danych co najmniej pomiędzy komputerem pacjenta (klienta), a pierwszym komponentem systemu, na którym są one przetwarzane. |
|  | System musi posiadać dedykowany moduł obsługi uprawnień, pozwalający na tworzenie i przydzielanie uprawnień użytkownikom osobowym, jak i innym systemom informatycznym (np. zintegrowanym z nim aplikacjom). |
|  | System musi umożliwiać udostępnianie danych medycznych (w tym dokumentacji medycznej) tylko dla autoryzowanych użytkowników. Użytkownik autoryzowany to osoba, której tożsamość została potwierdzona przez pracownika szpitala. |
| **Rejestracja i dostęp do portalu pacjenta (ePacjent)** |
|  | System musi umożliwiać samodzielne utworzenie konta w portalu. |
|  | Rejestracja do portalu udostępniana jest pacjentom w postaci odnośnika na stronie internetowej Zamawiającego. Po samodzielnym utworzeniu konta użytkownik posiada dostęp do portalu z określonym poziomem uprawnień. |
|  | Rejestracja konta użytkownika, który jest lub potencjalnie będzie pacjentem jednostki: |
|  | - system musi umożliwiać rejestracje podstawowych danych pacjenta tj.: |
|  | -- imię, nazwisko, |
|  | -- dane identyfikacyjne pacjenta: nr PESEL albo numer ewidencyjny lub numer dokumentu tożsamości nadane we wskazanym kraju (w przypadku rejestracji obcokrajowców), |
|  | - system musi umożliwiać rejestrację adresu e-mail użytkownika portalu, o ile weryfikowany jest taki kanał komunikacyjny, |
|  | - system musi umożliwiać rejestrację nr telefonu komórkowego użytkownika portalu, o ile weryfikowany jest taki kanał komunikacyjny, |
|  | - system podczas rejestracji użytkownika musi wymuszać akceptację regulaminu portalu, oraz zgody na przetwarzanie danych osobowych zgodnie z Ustawą z dnia 10 maja 2018 roku o Ochronie Danych Osobowych (tekst jednolity: Dz. U. 2018, poz. 1000). |
|  | - system umożliwia utworzenie konta dla którego:  |
|  | -- możliwe jest w zależności od ustawień systemu: wymuszenie zgodności nazwy użytkownika (loginu) z podanym adresem e-mail (o ile jest rejestrowany) |
|  | -- system umożliwia podanie i powtórzenie hasła do konta oraz weryfikuje poprawność podanego hasła z zadaną polityką. |
|  | Rejestracja konta użytkownika reprezentującego swojego podopiecznego: |
|  | - system umożliwia rejestrację konta użytkownika poprzez podanie jego imienia, nazwiska, danych kontaktowych (w zależności od przyjętego kanału komunikacji e-mail lub SMS), nazwy użytkownika i hasła, |
|  | - system umożliwia rejestrację danych podopiecznego użytkownika analogicznie do danych pacjenta. |
|  | System umożliwia weryfikację podanego w czasie rejestracji konta kanału komunikacyjnego: |
|  | -- e-mail, poprzez przesłanie na podany adres wiadomości zawierającej odnośnik z wygenerowanym kodem potwierdzenia autentyczności adresu e-mail, |
|  | -- SMS, poprzez przesłanie na podany nr telefonu wiadomości zawierającej kod potwierdzenia autentyczności podanego numeru; system udostępnia funkcję umożliwiającą wprowadzenie nr telefonu oraz przesłanego kodu. |
|  | System blokuje możliwość zalogowania się użytkownika, który nie potwierdził żadnego kanału komunikacyjnego. |
|  | System przypisuje zarejestrowanemu użytkownikowi predefiniowane uprawnienia do dostępnych funkcji, po potwierdzeniu kanału komunikacyjnego. |
|  | System udostępnia funkcję logowania do portalu, w ramach której, w zależności od przyjętej polityki bezpieczeństwa, mogą być weryfikowane następujące parametry: |
|  | -- wymuszenie zmiany hasła użytkowników, którzy pierwszy raz logują się do systemu, |
|  | -- wymuszenie zmiany hasła po upłynięciu określonego czasu od jego ostatniej zmiany, |
|  | System musi umożliwiać zmianę hasła użytkownika. |
|  | System podczas zmiany hasła musi weryfikować jego poprawność względem przyjętej polityki, w ramach której możliwe jest określenie: minimalnej długości hasła, minimalnej liczby wielkich liter, cyfr, znaków specjalnych, liczby niepowtarzających się kolejnych haseł użytkownika. |
|  | System udostępnia funkcję logowania do portalu, w ramach której, w zależności od przyjętej polityki bezpieczeństwa, mogą być weryfikowane następujące parametry:-- czasowe zablokowanie konta użytkownika po przekroczeniu określonej liczby nieudanych logowań. |
|  | System musi umożliwiać z poziomu systemu HIS: |
|  | - założenie konta użytkownika rejestracji on-line, |
|  | - rejestrację pacjentów związanych z kontem rejestracji on-line (właściciel konta lub jego podopieczni), |
|  | - autoryzację konta użytkownika (potwierdzenie faktu sprawdzenia tożsamości użytkownika rejestracji on-line) oraz jego uprawnień do reprezentowania podopiecznych. |
|  | Rejestracja konta użytkownika, który jest lub potencjalnie będzie pacjentem jednostki:* system umożliwia utworzenie konta, dla którego:
* możliwe jest wygenerowanie łatwej do zapamiętania unikalnej nazwy użytkownika (np. pierwsza litera imienia + nazwisko + opcjonalnie nr kolejny użytkownika)
* możliwe jest wprowadzenie przez rejestrującego własnej nazwy użytkownika z kontrolą jej unikalności,
 |
| **e-Zgoda** |
|  | Elektroniczny formularz umożliwiający przygotowanie oświadczenia na etapie przygotowania do wizyty przez pacjenta w domu a następnie podpisanie go i złożenie już gotowego w trakcie wizyty |
|  | Możliwość przesłania dokumentu podpisanego podpisem elektronicznym |
| **e-Rejestracja** |
|  | System musi umożliwiać pacjentom rezerwację terminów wizyt w jednostce Zamawiającego oraz anulowanie wcześniej dokonanych rezerwacji. |
|  | System umożliwia pacjentom wyszukiwanie usługi medycznej związanej z planowaną wizytą; wyszukiwanie usługi może odbywać się z wykorzystaniem następujących kryteriów: |
|  | -- nazwy usługi (poprzez podanie dowolnego ciągu znaków zawierającego się w nazwie usługi), |
|  | -- nazwy jednostki organizacyjnej szpitala, w której udzielana jest oczekiwana usługa, |
|  | -- imienia, nazwiska, tytułu naukowego i specjalności lekarza udzielającego oczekiwanej usługi. |
|  | System umożliwia wybór jednostki organizacyjnej, jeżeli usługa udzielana jest w wielu miejscach. |
|  | System umożliwia wybór personelu/lekarza udzielającego usługi medycznej, jeżeli jest dostępny dla danej usługi. |
|  | System umożliwia przegląd dostępnych dla rezerwacji internetowej terminów wizyt związanych z udzieleniem wybranej usługi medycznej oraz wybór wskazanego terminu. Po wybraniu terminu system blokuje możliwość wyboru tego terminu przez innych użytkowników zarówno systemu rejestracji on-line jak i systemu szpitalnego. |
|  | System umożliwia prezentację szczegółowych danych planowanej wizyty, tj.: |
|  | -- wybranej usługi medycznej, w tym informacji o warunkach udzielenia usługi, |
|  | -- danych adresowych miejsca udzielenia usługi, |
|  | -- danych wybranego personelu/lekarza udzielającego usługi. |
|  | System umożliwia lub wymusza (w zależności od konfiguracji dla danej usługi) rejestrację danych skierowania, w przypadku rezerwacji terminu dotyczącego świadczeń wymagających skierowania. |
|  | System umożliwia dodatkowe potwierdzenie autentyczności użytkownika rezerwującego termin wizyty poprzez przesłanie na podany nr telefonu kodu potwierdzającego oraz wymuszenie wprowadzenia tego kodu w kontekście rezerwacji wizyty. |
|  | System umożliwia przegląd zaplanowanych wizyt pacjenta. |
|  | System umożliwia prezentację szczegółowych danych zaplanowanej wizyty tj.: |
|  | - informacji o usłudze medycznej wraz z warunkami udzielenia usługi, |
|  | - danych teleadresowych miejsca udzielenia usługi, |
|  | - informacji o personelu udzielającym usługi (o ile jest wybrany na etapie rezerwacji terminu wizyty), |
|  | - planowanego terminu wizyty. |
|  | System umożliwia anulowanie rezerwacji wskazanego terminu wizyty. |
|  | System automatycznie usuwa rezerwacje terminów wizyt, które nie zostały potwierdzone kodem przesłanym przez SMS po upłynięciu zdefiniowanego przedziału czasu. |
|  | System integruje się on-line z systemem HIS w zakresie: |
|  | -- pobierania dostępnych terminów udzielenia wybranych świadczeń, |
|  | -- rezerwacji terminu wybranego świadczenia wraz z rejestracją danych skierowania, o ile są one wprowadzone przez pacjentów, |
|  | -- anulowania terminów zaplanowanych wizyt, |
|  | -- pobierania informacji o planowanych terminach wizyt. |
|  | System musi umożliwiać prezentację informacji o udzielonych świadczeniach opieki zdrowotnej oraz wpisach do list oczekujących (moje świadczenia) tj.: |
|  | - system prezentuje informacje o udzielonych świadczeniach opieki zdrowotnej – pobytach na oddziałach szpitalnych, udzielonych poradach, wykonanych badaniach, |
|  | - system prezentuje informacje o wpisach pacjentów na listy oczekujących. |
|  | System musi prezentować informacje o wystawionych dokumentach sprzedaży dotyczących udzielonych świadczeń medycznych w postaci: |
|  | - data udzielenia świadczenia, |
|  | - nazwa świadczenia, |
|  | - nr dokumentu sprzedaży, |
|  | - kwota do zapłaty, |
|  | - status płatności (opłacona/nieopłacona). |
|  | System umożliwia zrealizowanie płatności on-line za udzielone świadczenie. |
|  | System musi umożliwiać przegląd zrealizowanych badań, zarejestrowanych w systemie HIS, których wyniki zostały udostępnione do przeglądu w portalu. Możliwe jest filtrowanie badań wg dat realizacji oraz wyszukiwanie wg nazwy badania. |
|  | System musi prezentować wyniki wybranych badań laboratoryjnych. |
|  | System musi umożliwiać pobranie elektronicznych dokumentów medycznych pacjenta, zarejestrowanych w Repozytorium EDM. |
|  | System integruje się on-line z systemem HIS w zakresie pobierania informacji o udzielonych świadczeniach medycznych (system nie tworzy własnego, oddzielnego repozytorium danych medycznych). |
|  | System integruje się on-line z Repozytorium Elektronicznej Dokumentacji Medycznej (Repozytorium EDM w systemie HIS) w zakresie pobierania informacji o dostępnej elektronicznej dokumentacji medycznej (system nie tworzy własnego, oddzielnego repozytorium meta danych dokumentów i dokumentów w postaci elektronicznej). |
|  | System integruje się on-line z modułem rozliczeń komercyjnych w zakresie pobrania informacji o wystawionych dokumentach sprzedaży z uwzględnieniem aktualizacji statusu płatności po zrealizowaniu płatności internetowej. |
|  | System musi umożliwiać ograniczenie udostępnianych dokumentów do dokumentów podpisanych bezpiecznym podpisem cyfrowym. |
|  | System musi umożliwiać ograniczenie udostępnianych dokumentów do dokumentów wybranych typów. |
| **e-Korespondencja** |
|  | System umożliwia obsługę wiadomości przekazywanych do jednostki Zamawiającego, tj.: |
|  | - system umożliwia rejestrację wiadomości przekazywanej do szpitala, |
|  | - system umożliwia zdefiniowanie kategorii rejestrowanych wiadomości (np. skarga, pochwała itp.). |
| **e-Ankieta** |
|  | System musi umożliwiać przeprowadzenie badań satysfakcji pacjentów poprzez udostępnienie ankiet związanych z udzielonymi świadczeniami medycznymi, automatyczne definiowanie szablonów do przeprowadzania analiz i generowania wykresów w zależności od zadanych parametrów. |
|  | System musi przesyłać pacjentom wiadomości z prośbą o wypełnienie ankiety z wykorzystaniem wybranego kanału komunikacyjnego (SMS, e-mail, wiadomość portalowa). System umożliwia uruchomienie ankiety do wypełnienia poprzez kliknięcie odnośnika przesłanego w wiadomości e-mail. |
|  | System musi umożliwiać udostępnienie różnych ankiet dla określonych usług medycznych. |
|  | System musi umożliwiać pacjentom wypełnienie zdefiniowanej ankiety dotyczącej udzielonego świadczenia medycznego. |
| **e-Wywiad lekarski** |
|  | System umożliwia pacjentom wypełnienie wywiadu lekarskiego w kontekście planowanej usługi medycznej. |
|  | System zapisuje wywiad lekarski w postaci dokumentu określonego typu w Repozytorium EDM. |
|  | System musi umożliwiać wysyłanie wiadomości z prośbą o uzupełnienie wywiadu lekarskiego w zadanym czasie przed planowaną datą udzielenia świadczenia. |
|  | System umożliwia pacjentowi modyfikację wywiadu lekarskiego, który rejestrowany jest jako kolejna wersja dokumentu w Repozytorium EDM. |
|  | System weryfikuje kompletność zebranego wywiadu lekarskiego, rozumianą jako udzielenie odpowiedzi na wszystkie pytania jej wymagające. |
|  | System integruje się z systemem HIS w zakresie rejestracji dokumentu e-wywiadu lekarskiego w Repozytorium EDM systemu HIS. |
| **e-Załącznik** |
|  | System musi umożliwiać pacjentom zarejestrowanie załącznika w kontekście planowanej wizyty. |
|  | System musi umożliwiać rejestrację załącznika jako dokument w Repozytorium EDM systemu HIS. |
| **e-Zgody** |
|  | System musi umożliwić wypełnienie elektronicznego formularza zgody na dostęp do dokumentacji medycznej pacjenta oraz wyznaczenia osoby upoważnionej do uzyskiwania informacji o jego stanie zdrowia. |
|  | System musi umożliwiać wypełnienie formularza oświadczenia przez pacjenta przed wizytą, podpisanie go profilem zaufanym e-PUAP i złożenie drogą elektroniczną za pośrednictwem portalu. |
|  | System musi umożliwić pacjentom nieposiadającym profilu zaufanego lub nie wyrażającym zgody na tę formę komunikacji wydruk wypełnionego formularza oświadczenia, w celu dostarczenia oryginału dokumentu w wersji papierowej w wybrany przez siebie sposób. |
|  | System musi umożliwić wymianę dokumentów typu skierowanie wg standardu opublikowanego przez CSiOZ, w ramach projektu P1. |
| **e-Recepta** |
|  | Usługa musi zostać udostępniona na stronie WWW Zamawiającego i być dostępna zarówno w sieci Internet jak i wewnętrznej każdej placówki Zamawiającego. |
|  | Usługa musi być dostępna dla każdego pacjenta posiadającego odpowiednie konto i uprawnionego do korzystania z usługi. |
|  | Usługa musi być możliwa do uruchomienia dla pacjentów na kiosku internetowym w placówce Zamawiającego. |
|  | Dostępność usługi e-Recepty musi być możliwa z poziomu stacji roboczych. |
|  | Usługa po dokonaniu wyboru usługi "wizyta receptowa" wymaga uzupełnienia w formularzu listy leków, na które powinny zostać wystawione recepty. |
|  | Usługa musi umożliwiać wymuszenie podania uzasadnienia wystawienia recepty |
|  | Recepty wystawiane są w systemie HIS |
|  | Usługa udostępnia pacjentowi dane wystawionych recept. |
|  | Usługa umożliwia wystawienie recepty papierowej do odbioru we wskazanym miejscu. |
|  | Usługa informuje pacjenta o dostępnych receptach z wykorzystaniem kanałów: SMS, email lub wiadomość na portalu |
|  | Pacjent musi mieć możliwość wglądu do listy swoich zarezerwowanych terminów zarówno tych zarezerwowanych online jak również zaplanowanych w systemie HIS – umówionych poprzez personel rejestracji placówki. |
|  | Pacjent musi mieć możliwość zmiany online terminu zaplanowanej wcześniej usługi poprzez wskazanie nowego terminu spośród dostępnych, a informacja o dokonanej zmianie terminu przez Pacjenta musi być dostępna w systemie HIS |
|  | Usługa musi umożliwić wysłanie do pacjenta potwierdzenia zmiany terminu wizyty na adres email i/lub SMS. |
|  | Usługa musi umożliwiać pacjentowi dokonanie odwołania zaplanowanej usługi, a informacja o odwołaniu musi być dostępna w systemie HIS. |
|  | System musi prowadzić dziennik logowań użytkowników do usługi e-Rejestracji. |
|  | System musi umożliwić bieżące śledzenie terminów rezerwowanych wizyt receptowych przez uprawnionego pracownika Zamawiającego. |
|  | Usługa umożliwia wysłanie recepty przygotowanej w systemie HIS do rejestru centralnego działającego w ramach projektu P1. |
|  | Usługa umożliwia pobranie identyfikatorów recepty nadanych przez system centralny: klucz pakietu recept, klucz recepty, kod recepty. |
|  | Usługa umożliwia sprawdzenie recept wystawionych pacjentowi. |
|  | Usługa musi zapewniać, dla uprawnionego personelu Zamawiającego, możliwość definiowania i aktualizacji grafików dostępności świadczonych usług medycznych, w tym możliwość ograniczenia rejestracji online do wybranych godzin oraz ograniczenia liczby jednocześnie wprowadzanych przez pacjenta rezerwacji wizyt receptowych w trybie rejestracji online (rejestracji w przód). |
|  | Usługa umożliwia wysłanie dokumentu anulowania wystawionej recepty. |
| **e-Administrator** |
|  | Przegląd i modyfikacja danych użytkowników. |
|  | Tworzenie grup użytkowników; przyporządkowanie użytkowników do grup. |
|  | Przydzielanie uprawnień i ról użytkownikom i grupom użytkowników. |
|  | Przegląd efektywnych uprawnień użytkownika wynikających z przynależności do grup użytkowników, przypisanych ról i praw. |
|  | Możliwość przydzielania uprawnień do zmieniających się w czasie zasobów. |
|  | Definiowanie polityk poziomu bezpieczeństwa hasła użytkownika, możliwość przypisania wskazanych polityk do użytkowników. |
|  | Kontrola złożoności hasła użytkownika zgodnie z przypisaną polityką poziomu bezpieczeństwa. |
|  | Dostępność interfejsu umożliwiającego integrację użytkowników z dotychczas użytkowanym systemem (interfejsy na poziomie bazy danych i języków wysokiego poziomu). |
|  | Dostępność interfejsu do kontroli praw przyznanych użytkownikom (interfejsy na poziomie bazy danych i języków wysokiego poziomu). |
|  | Dostępność interfejsu do zarządzania prawami przyznanych użytkownikom (interfejsy na poziomie bazy danych i języków wysokiego poziomu). |
|  | Użytkownicy systemu nie odpowiadają bezpośrednio użytkownikom systemu zarządzania bazą danych. |
|  | Możliwość delegowania uprawnień do administrowania uprawnieniami w poszczególnych podsystemach. |

#### Elektroniczna Dokumentacja Medyczna (repozytorium)

|  |  |
| --- | --- |
| **L.p.** | **Wymagania ogólne** **Parametry wymagane** |
|  | Aplikacja posiada interfejs funkcjonalny w technologii „lekkiego” klienta właściwej dla zapewnienia możliwości wykorzystywania do tego celu (dostęp) przeglądarek hipertekstowych (HTML); |
|  | Możliwość archiwizacji dokumentacji medycznej w postaci elektronicznej. |
|  | Możliwość archiwacji dokumentów złożonych, wieloczęściowych i przyrostowych tj. księgi |
|  | Możliwość obsługi załączników do dokumentów |
|  | Możliwość rejestracji dokumentów elektronicznych generowanych przez system medyczny w repozytorium dokumentacji elektronicznej |
|  | Możliwość rejestracji dokumentów elektronicznych utworzonych poza systemem HIS, manualna rejestracja dokumentów zewnętrznych |
|  | Cyfryzacja dokumentu papierowego i dołączanie go do dokumentacji elektronicznej |
|  | Możliwość exportu/importu dokumentu elektronicznego do/z pliku w formacie XML |
|  | Możliwość złożenia podpisu elektronicznego na dokumencie oraz na zbiorze dokumentów |
|  | Możliwość złożenia podpisu elektronicznego na zbiorze dokumentów |
|  | Możliwość znakowania czasem dokumentu |
|  | Możliwość wykonania kontrasygnaty |
|  | Możliwość weryfikacji podpisu |
|  | Możliwość weryfikacji integralności dokumentu |
|  | Możliwość wydruku dokumentu |
|  | Możliwość wyszukiwania dokumentów za pomocą zaawansowanych kryteriów oraz meta danych. |
|  | Możliwość wersjonowania przechowywanych dokumentów z dostępem do pełnej historii poprzednich wersji. |
|  | Repozytorium EDM musi umożliwiać: |
|  |  - rejestrację dokumentu |
|  |  - pobieranie dokumentów w formacie XML |
|  |  - pobieranie dokumentów w formacie PDF |
|  |  - wyszukiwanie materializacji dokumentów |
|  | System uprawnień pozwalający na precyzyjne definiowanie obszarów dostępnych dla danego użytkownika pełniącego określoną rolę. |
|  | Możliwość zarządzania uprawnieniami dostępu do określonych operacji w repozytorium. Przykłady uprawnień systemowych: uruchomienie systemu, zarządzanie uprawnieniami użytkowników, zarządzanie parametrami konfiguracyjnymi, zarządzanie typami dokumentów. |
|  | Możliwość zarządzania uprawnieniami do wykonywania operacji na poszczególnych typach dokumentów w ramach całej placówki lub poszczególnych jednostek organizacyjnych. Przykłady uprawnień do dokumentów: dodawanie dokumentów do repozytorium, odczyt dokumentu, podpisywanie dokumentu, znakowanie czasem dokumentu, import i eksport dokumentu, anulowanie dokumentu, wydruk dokumentu itd. |
|  | Możliwość definiowania nowych typów dokumentów obsługiwanych przez repozytorium dokumentów elektronicznych. |
|  | Zakłada się także możliwość indeksowania dokumentów, których elektroniczna postać nie jest przechowywana w systemie HIS - np. indeksowanie dokumentów papierowych, obrazów radiologicznych przechowywanych w PACS. |
|  | Indeksowane powinny być wszystkie wersje dokumentu |
|  | Indeks powinien uwzględniać rozdzielenie danych osobowych od danych medycznych |
|  | Możliwość indeksowania dokumentów w celu łatwego jej wyszukiwania wg zadanych kryteriów |
|  | Indeks dokumentacji powinien być zorientowany na informacje o dokumencie: autor, data powstania, rozmiar, typ, data powstania itp., oraz na informacje o zdarzeniach |
|  | System musi umożliwić udostępnianie dokumentacji: |
|  |  - w celu realizacji procesów diagnostyczno-terapeutycznych w ZOZ |
|  |  - pacjentom i ich opiekunom |
|  |  - podmiotom upoważnionym np. prokurator |
|  | System powinien umożliwiać wymianę dokumentacji medycznej w ramach Systemu Informacji Medycznej: |
|  |  - bezpośrednio pomiędzy jednostkami ochrony zdrowia |
|  |  - za pośrednictwem systemów regionalnych |
|  |  - z wykorzystaniem platformy P1. |
|  | Podpis cyfrowy |
|  | System musi umożliwiać złożenie podpisu cyfrowego na przekazanych dokumentach oraz zapewnia: |
|  | - możliwość podpisywania pojedynczych dokumentów, |
|  | - możliwość podpisywania grupy dokumentów z jednokrotnym zapytaniem o PIN, |
|  | - możliwość określenia formatu podpisu (zewnętrzny lub otaczający/otaczany). |
|  | Dostęp do całości dokumentacji przechowywanej w EDM: |
|  | - z poziomu wbudowanych w systemy medyczne mechanizmów |
|  | - z poziomu dedykowanego interfejsu  |
|  | Repozytorium EDM musi współdzielić z HIS: |
|  | - słownik jednostek organizacyjnych |
|  | - rejestr użytkowników |
|  | - rejestr pacjentów |

#### LIS – integracja HIS-LIS

Zamawiający używa obecnie Oprogramowania CENTRUM, autorstwa firmy Marcel.

|  |  |
| --- | --- |
| Lp. | **Wymagania ogólne** **Parametry wymagane** |
|  | Integracja z wykorzystaniem standardu HL7 |
|  | Segmenty wspólne dla komunikatów wysyłanych przez HIS i LIS |
|  | Segment MSH - nagłówek komunikatu obejmujący: |
|  |  - Kod systemu nadawcy |
|  |  - Kod systemu adresata |
|  |  - data i czas utworzenia komunikatu |
|  |  - typ komunikatu |
|  |  - unikatowy identyfikator komunikatu |
|  |  - tryb interpretacji komunikatu |
|  |  - wersja standardu HL7 |
|  |  - potwierdzenia: transportowe i aplikacyjne |
|  |  - stosowany system kodowania znaków |
|  |  - język komunikacji |
|  | **Dane przesyłane z systemu HIS** |
|  | Segment PID - dane demograficzne pacjenta obejmujące: |
|  |  - PESEL |
|  |  - Imiona i nazwisko pacjenta, nazwisko rodowe |
|  |  - identyfikator pacjenta |
|  |  - data urodzenia |
|  |  - płeć |
|  |  - adres |
|  | Segment PV1 - informacje o wizycie lub pobycie pacjenta, obejmujący: |
|  |  - rodzaj pobytu: pobyt na IP, wizyta ambulatoryjna, hospitalizacja |
|  |  - jednostka organizacyjna |
|  |  - rodzaj świadczenia |
|  |  - identyfikator pobytu, np. nr księgi |
|  | Segment IN1 - informacje o ubezpieczeniu pacjenta obejmujące: |
|  |  - identyfikator płatnika |
|  |  - rodzaj skierowania |
|  | Segment ORM^O01 - dane zlecenia obejmujące: |
|  |  - nr zlecenia |
|  |  - planowana data wykonania, pilność |
|  |  - datę i czas zlecenia |
|  |  - dane osoby zlecającej |
|  |  - identyfikator zlecanego badania |
|  |  - dane pobrania tj.: osoba pobierająca, moment pobrania, pobrany materiał (rodzaj i numer próbki) |
|  |  - rozpoznanie ze zlecenia |
|  |  - komentarz do zlecenia |
|  |  - dane badania (kod i nazwa badania) |
|  | Anulowanie zlecenia |
|  | Modyfikacja zlecenia |
|  | **Dane przesyłane z systemu LIS** |
|  | Segment ORU^R01 - wynik obejmujący: |
|  |  - status wyniku |
|  |  - dane zlecenia |
|  |  - kod wykonanego badania |
|  |  - datę wykonania |
|  |  - dane personelu wykonującego: lekarz wykonujący, lekarz opisujący, lekarz konsultujący, technik, osoba autoryzująca |
|  |  - wartość wyniku |
|  |  - jednostka miary i wartość referencyjna, przekroczenie normy |
|  | Odnośniki (załączniki) do wyników badań |
|  | Wyniki badań dozleconych (dodatkowych) |
|  | Wyniki badan nie zleconych przez HIS |
|  | Anulowanie wyniku |
|  | Zmiana wyniku |

### Migracja danych

Zamawiający oczekuje (w przypadku wymiany systemu na nowy) migracji wszystkich danych z użytkowanych dotychczas systemów do nowego SSI.

Systemy podlegające ewentualnej migracji: AMMS/Infomedica Asseco Poland S.A. (część medyczna).

Informacje o bazie danych HIS:

|  |  |  |
| --- | --- | --- |
| L.p. | Zapytanie | Odpowiedź |
|  | Ilość baz danych | 1 |
|  | Rodzaj baz danych | złożona relacyjna |
|  | Struktura poszczególnych baz danych | relacyjna |
|  | Rodzaje i ilość tabel | tabele zgodne z bazą danych Oracle - 1280 tabel |
|  | Zakres danych w tabelach | dane medyczne z lat 2001 - 2020 |
|  | Opis danych w tabelach | pacjenci, słowniki, dane rozliczeniowe, dane statystyczne, kolejki oczekujących |
|  | Relacje pomiędzy danymi | w podmiocie medycznym przyjęto taką relację między danymi, że nigdy jedna informacja, nie jest zapisywana w bazie dwa razy |
|  | Zainstalowane procedury po stronie serwera bazy danych | procedura bezpieczeństwa, procedura kontroli spójności danych |
|  | Logiczne powiązania pomiędzy tabelami w bazie danych | brak |
|  | Rozmiar baz danych | 2 TB |
|  | Sposób migracji | Do decyzji wykonawcy |
|  | Informacje na temat spójności danych | dane są spójne |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Lp. | Zakres danych | Środowisko bazodanowe | Ilość instancji | Czy istnieje możliwość wyeksportowania wskazanego zakresu danych do formatu zewnętrznego?(TAK / NIE) | Jeśli istnieje możliwość wyeksportowania wskazanego zakresu danych, jaki jest to format eksportu? |
| 1 | Dane o pacjentach i ich opiekunach | oracle | 1 | TAK we własnym zakresie przez wykonawcę | XML, CSV |
| 2 | Słownik personelu | oracle | 1 | Jw. | XML, CSV |
| 3 | Słownik jednostek kierujących | oracle | 1 | Jw. | XML, CSV |
| 4 | Słownik lekarzy kierujących | oracle | 1 | Jw. | XML, CSV |
| 5 | dane o płatnikach i umowach | oracle | 1 | Jw. | XML, CSV |
| 6 | dane statystyczne rozliczonych pacjentów do NFZ | oracle | 1 | Jw. | XML, CSV, format eksportu NFZ |
| 7 | Dane rozliczeniowe z możliwością wykonania korekt wstecznych według wymogów NFZ | oracle | 1 | Jw. | XML, CSV, format eksportu NFZ |
| 8 | Dane opisowe wyników pacjenta w tym dane wyniki laboratoryjne i diagnostyczne | oracle | 1 | Jw. | XML, CSV |

### Warunki przeniesienia danych

1. Zamawiający informuje, że nie posiada dokumentacji struktur baz danych posiadanych systemów. Na prośbę Wykonawcy, na podstawie art. 9a ust. 2 ustawy Pzp, Zamawiający umożliwi Wykonawcy dostęp do baz danych posiadanych systemów informatycznych (wizja lokalna) i udzieli wsparcia Wykonawcy w dokonaniu przeniesienia danych poprzez: nadanie wskazanym pracownikom Wykonawcy niezbędnych uprawnień do pracy w systemie oraz do zapoznania się ze strukturami tabel w bazach danych posiadanych systemów. Dostęp do baz danych posiadanych systemów informatycznych i ich dokumentacji, może być udzielony po uprzednim uzgodnieniu terminu wizyty Wykonawcy i po uregulowaniu zasad dostępu do chronionych danych osobowych. Zamawiający umożliwi Wykonawcy przeprowadzenie wizji lokalnej w dni robocze, pomiędzy godziną 8:00 a 15:00. Osobą odpowiedzialną po stronie Zamawiającego za uzgodnienie terminu wizji lokalnej jest – Kierownik Działu Informatyki.
2. Zamawiający udostępni Wykonawcy, z którym podpisze umowę, posiadane instrukcje obsługi posiadanych systemów.
3. Wykonawca ponosi odpowiedzialność za ewentualne szkody, wyrządzone przez jego pracowników, powstałe w wyniku działań prowadzonych przez Wykonawcę na bazach danych posiadanych systemów.
4. Informacje uzyskane przez Wykonawcę w toku wykonania czynności, o których mowa w art.75 ust.2 pkt 3 ustawy Prawo autorskie (Dz.U. 2006, nr 90, poz.631), stanowią tajemnicę przedsiębiorstwa w rozumieniu Ustawy o zwalczaniu nieuczciwej konkurencji z dnia 16 kwietnia 1993 r. (Dz.U. Nr 47, poz. 211 z późn. zm.) i podlegają ochronie w niej przewidzianej.

### Instruktaże stanowiskowe

1. Z uwagi na to, iż w ramach projektu planuje się wdrożenie specjalistycznego oprogramowania i aplikacji, konieczne jest przeszkolenie personelu Zamawiającego. W związku z tym w ramach tego zadania zostaną zrealizowane instruktaże stanowiskowe.
2. Wykonawca przeprowadzi instruktaże stanowiskowe w siedzibie Zmawiającego. Zamawiający udostępni pomieszczenie celem przeprowadzenia instruktaży stanowiskowych.
3. Na podstawie przekazanego przez Zamawiającego wykazu osób oraz przewidywanego terminu i czasu instruktażu stanowiskowego, Wykonawca zaproponuje harmonogram jak i podział na grupy.
4. Szczegółowy harmonogram realizacji instruktaży zostanie uzgodniony na etapie Analizy Przedwdrożeniowej.
5. Harmonogramy instruktaży muszą umożliwiać informatykom Zamawiającego obecność na zajęciach z danego tematu przeznaczonych dla innych grup zawodowych, z zastrzeżeniem, że na jednych zajęciach z danego tematu może być obecny co najmniej 1 informatyk.
6. Wykonawca nie ponosi odpowiedzialności za brak uczestnictwa użytkowników w instruktażach stanowiskowych.
7. Instruktaże stanowiskowe użytkowników oprogramowania SSI i administratora będą musiały spełniać minimum następujących wymagania:
* zajęcia powinny odbywać się w godzinach od godz. 8.00 do 15.00,
* zajęcia nie będą mogły trwać dłużej niż 6 godzin dziennie,
1. Za skuteczne przeprowadzenie instruktażu stanowiskowego uważa się dostępność w ustalonym miejscu i terminie przedstawicieli Wykonawcy, gotowych przeprowadzić instruktaż zgodnie z ustalonym harmonogramem.
2. Wykonawca w ramach instruktażu stanowiskowego przekaże instrukcje do wdrożonego Systemu oraz materiały szkoleniowe. Instruktaże stanowiskowe będą prowadzone w języku polskim
3. W ramach przeprowadzonych instruktaży stanowiskowych wymaga się:
* przekazania wiedzy niezbędnej do poprawnego użytkowania wdrożonego systemu, jego zakresu funkcjonalnego,
* przekazania wiedza w zakresie tworzenia i gromadzenia informacji, tworzeniem i gromadzeniem dokumentów, wykonywaniem analiz, sprawozdań i raportów.
1. Zakres instruktaży stanowiskowych musi objąć teorię i praktykę (musi być zapewniona odpowiednia liczba ćwiczeń – minimum w stosunku 50% / 50%) tak, aby personel Zamawiającego mógł podjąć samodzielnie działania użytkowania wdrożonego oprogramowania SSI.
2. Instruktaże stanowiskowe będą prowadzone w dwóch kategoriach:

a) dla użytkowników oprogramowania SSI – **150 godzin**

b) dla administratorów – **200 godzin**

1. Szacowana liczba pracowników Zamawiającego planowanych do instruktaży stanowiskowych 191 osób personelu Zamawiającego i 9 administratorów. Zatrudnienie personelu na dzień 31.12.2019 kształtowało się następująco:
* lekarze - 466
* farmaceuci - 8
* fizjoterapeuci/logopedzi - 132
* pielęgniarki - 996
* położne - 134
* technicy - 59
* technicy RTG - 33
* sekretarki - 133
* ratownicy medyczni - 25
* obsługa – 11
* informatycy - 9
1. Po ukończeniu instruktaży stanowiskowych uczestnicy mają w szczególności umieć:
* posługiwać się w pełni samodzielnie wdrożonym oprogramowaniem SSI i jego modułami odpowiednio do swojej roli, a także znać i rozumieć ich funkcjonowanie w Systemie.
1. Administratorzy po zakończeniu instruktaży muszą w szczególności umieć
* wykonywać czynności administracyjne a także instalacji oprogramowania systemowego i narzędziowego oraz oprogramowania SSI, znać i umieć realizować procedury backupu, znać wytyczne w zakresie polityki bezpieczeństwa i umieć je stosować. Ponadto powinni znać typowe zagrożenia i problemy związane z funkcjonowaniem Systemu, a także sposoby ich wykrywania oraz przeciwdziałania. Powinni umieć instalować, konfigurować, rekonfigurować, monitorować i prawidłowo eksploatować dostarczony Sprzęt i Oprogramowanie, jak również znać jego wdrożoną konfigurację.
1. W przypadku obowiązywania zasad i ograniczeń wynikających z rozporządzenia Ministra Zdrowia obostrzeń dotyczących zakazu zgromadzeń w związku z sytuacją epidemiologiczną COVID-19, Zamawiający dopuszczę przeprowadzenie instruktaży stanowiskowych on-line **dla użytkowników oprogramowania SSI.**
2. Instruktaże stanowiskowe on-line powinny być prowadzone w technologii transmisji audio-wideo w czasie rzeczywistym, tzn. technologią typu „Streaming” umożliwiającą przesyłanie takich danych jak fonia, wizja i tekst „na żywo” dzięki czemu uczestnik otrzymuje pełnowartościowe szkolenie:
* fonia / głos – słyszy lektora prowadzącego szkolenie „na żywo”
* wizja /wideo – widzi lektora prowadzącego szkolenie „na żywo”
* pokaz slajdów, prezentacji, widoku ekranu – całą prezentację widzi u siebie na ekranie.

Instruktaże stanowiskowe on-line muszą umożliwiać pełną interakcję zarówno z prowadzącym jak i z innym uczestnikami instruktażu, poprzez:

1. dostęp do czatu z możliwością zadawania pytań oraz udzielania odpowiedzi,
2. przeprowadzenia ankiet on-line.

Zakres instruktaży stanowiskowych on-line musi obejmować teorię, czyli prezentację oraz praktykę, tj. wykonywania ćwiczeń przez uczestników, zgodnie z pkt 11 niniejszego rozdziału.

Wykonawca jest odpowiedzialny za organizację instruktaży stanowiskowych on-line, w tym co najmniej: zapewnienie sprzętu, oprogramowania oraz transmisji do przeprowadzenia instruktaży, w miejscu wyznaczonym przez Zamawiającego.

# Gwarancja

1. Wykonawca w ramach realizacji Przedmiotu Zamówienia udzieli Zamawiającemu gwarancji jakości (dalej zwanej „gwarancją”) na niniejszy przedmiot zamówienia:
2. **Dostawa i wdrożenie Infrastruktury serwerowej i sieciowej wraz z oprogramowaniem systemowym i narzędziowym oraz Szpitalnym Systemem Informatycznym:**
3. Infrastruktura serwerowa:

|  |  |  |
| --- | --- | --- |
| **Poz. SOPZ** | **Opis** | **Okres gwarancji (minimalny)\*** |
| II.1.1 | Serwer wirtualizacyjny\*\* | **60 miesięcy**  |
| II.1.2 | Serwer do kopii (backup)\*\* | **60 miesięcy**  |
| II.1.3 | Serwer bazodanowy\*\* | **60 miesięcy**  |
| II.1.4 | Serwer bazodanowy zapasowy\*\* | **60 miesięcy** |
| II.1.5 | Macierz główna\*\* | **60 miesięcy** |
| II.1.6 | Macierz zapasowa\*\* | **60 miesięcy** |
| II.1.7 | Macierz backup/serwer\*\* | **60 miesięcy** |
| II.1.8 | Biblioteka LTO | **60 miesięcy** |
| II.1.9 | Przełącznik zasobowy do macierzy | **60 miesięcy** |
| II.1.10 | Szafa rack | **60 miesięcy** |
| II.1.11 | Zasilacz awaryjny UPS | **60 miesięcy** na zasilacz awaryjny UPS **24 miesiące** na akumulatory |

**\*** 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.

1. Oprogramowanie systemowe i narzędziowe w zakresie:

|  |  |  |
| --- | --- | --- |
| **Poz. SOPZ** | **Opis** | **Okres gwarancji (minimalny)**  |
| **Rozdział II.2** | **Oprogramowanie systemowe i narzędziowe** |   |
| II.2.1 | Serwerowy system operacyjny | **36 miesięcy** |
| II.2.2 | Licencje dostępowe serwera | **36 miesięcy** |
| II.2.3 | Oprogramowanie bazodanowe | **36 miesięcy** |
| II.2.4 | Oprogramowanie systemowe storage | **36 miesięcy** |
| II.2.5 | Oprogramowanie systemowe Load Balancer | **36 miesięcy** |
| II.2.6 | Oprogramowanie wirtualizacyjne | **36 miesięcy** |
| II.2.7 | Oprogramowanie do robienia kopii zapasowych | **36 miesięcy** |

Wykonawca udzieli i będzie realizował gwarancję w poniższym zakresie:

1. Zapewnienia prawidłowej pracy w/w oprogramowania systemowego i narzędziowego w ramach posiadanych licencji i wsparć producenta na poszczególne elementy środowiska.
2. Identyfikacji i diagnoz zgłoszonych problemów.
3. Wykonanie niezbędnych zmian konfiguracji systemów w celu usunięcia problemu, o ile takie będą konieczne.
4. Działań prewencyjnych w celu zapobiegania awariom.
5. modernizacja sieci LAN w zakresie dostawy i wdrożenia sieciowej infrastruktury sprzętowej:

|  |  |  |
| --- | --- | --- |
| **Poz. SOPZ** | **Opis** | **Okres gwarancji (minimalny)** |
| II.3.1 | Przełącznik LAN: |
| Przełącznik zarządzający | **60 miesięcy** gwarancji producentaobejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) |
| II.3.2 | Przełącznik rdzeniowy | **60 miesięcy** gwarancji producentaobejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory), w trybie Next Business Day |
| II.3.3 | Przełącznik dostępowy | **60 miesięcy** gwarancji producentaobejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) |

1. dostawa i wdrożenie Szpitalnego Systemu Informatycznego:

|  |  |  |
| --- | --- | --- |
| **Poz. SOPZ** | **Opis** | **Okres gwarancji****(minimalny)** |
| II.4.5   | System HIS – część medyczna | **36 miesięcy** |
| System LIS - integracja |
| Elektroniczna Dokumentacja Medyczna |
| e-Usługi – eRejestracja On-Lina z Portalem |

1. Bieg terminów gwarancji określonych w ust. 1 będą rozpoczynać się z dniem podpisania Protokołu Odbioru Końcowego bez uwag przez Zamawiającego.
2. Naprawy gwarancyjne muszą być realizowane przez serwis producenta lub Autoryzowanego Partnera Serwisowego Producenta z wyłączeniem pozycji wskazanych w pkt 1 b) - Oprogramowanie systemowe i narzędziowe.

### Zakres usług gwarancyjnych dostarczonego oprogramowania aplikacyjnego.

|  |  |
| --- | --- |
| **Nazwa Usługi** | **Przedmiot Usługi** |
| Zakres usług gwarancyjnych | Gotowość Wykonawcy do usuwania błędów oprogramowania aplikacyjnego.Usługa realizowana za pośrednictwem Wykonawcy przez producenta oprogramowania aplikacyjnego.Realizacja usługi 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. W ramach usługi Wykonawca zagwarantuje:* prowadzenie rejestru zgłaszanych przez użytkowników błędów ww. oprogramowania aplikacyjnego
* wprowadzanie do ww. oprogramowania aplikacyjnego nowych funkcji oraz usprawnień już istniejących, stanowiących wynik inwencji twórczej producenta,
* 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.
* wprowadzanie do oprogramowania aplikacyjnego zmian wymaganych przez wyszczególnione poniżej organizacje, w stosunku do których Zamawiający ma obowiązek prowadzenia sprawozdawczości, w szczególności:
* Ministerstwa Zdrowia,
* NFZ,
* Centrów Zdrowia Publicznego,
* Ministerstwa Finansów.
* wprowadzanie w trybie pilnym do ww. oprogramowania aplikacyjnego zmian i poprawek usuwających stwierdzone błędy i luki we wbudowanych mechanizmach i funkcjach zabezpieczeń,
* gotowość do odpłatnego wykonania na zlecenie Zamawiającego zaproponowanych przez niego modyfikacji ww. oprogramowania aplikacyjnego.
 |
| Konsultacje | Gotowość do świadczenia Zamawiającemu usługi pomocy techniczneji eksploatacyjnej w odniesieniu do ww. oprogramowania aplikacyjnego. |

###

### Usługi gwarancyjne

1. W okresie gwarancji Wykonawca będzie zobowiązany do nieodpłatnego usuwania Wad Przedmiotu Zamówienia rozumianych jako Awaria lub Błąd lub Usterka zgodnie z definicjami, jak poniżej:
2. **Awaria -** Kategoria Wady w Oprogramowaniu lub Oprogramowaniu SSI lub 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.
3. **Błąd** - Należy przez to rozumieć Wadę Oprogramowania lub Oprogramowania SSI oznaczającą jego funkcjonowanie niezgodne z opisem w Dokumentacji oraz SOPZ, powodujące błędne zapisy w bazie danych lub uniemożliwiające działanie mniej istotnej funkcjonalności w Systemie.
4. **Usterka -** Należy przez to rozumieć kategorię Wady w Oprogramowaniu lub Oprogramowaniu SSI lub Infrastrukturze Sprzętowej oznaczającą funkcjonowanie niezgodne z opisem Dokumentacji oraz SOPZ, nie wpływającą istotnie na funkcjonowanie dostarczanego rozwiązania u Zamawiającego, utrudniającą pracę Użytkownikowi Zamawiającego.
5. Przyjęcie zgłoszenia Wady przez Wykonawcę, odbywać się będzie poprzez dostępny on-line System Zgłaszania i przyjmowania uwag oraz Wad (dalej zwany SZ) przy czym:
6. System Zgłoszeń dostarczy Wykonawca (będzie on utrzymywany i administrowany przez Wykonawcę), wpis zgłoszenia do SZ będzie dokonywał Zamawiający,
7. 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.
8. W przypadku, w którym wykonanie Umowy związane będzie z modernizacją lub rozbudową istniejącego oprogramowania, gwarancja obejmuje całość oprogramowania modernizowanego lub rozbudowywanego.
9. Gwarancja musi zapewniać wymianę uszkodzonego sprzętu, kabli i elementów oraz zapewniać dostęp do aktualizacji oprogramowania, bez wiedzy i wsparcia technicznego producenta.
10. W ramach gwarancji Wykonawca będzie świadczył następujące usługi:
11. Usuwanie Wad w dostarczonym Przedmiocie Zamówienia w przypadku stwierdzenia przez Zamawiającego Wady w jego działaniu, w terminach określonych poniżej:

**Tabela 1. Usługi gwarancji dla Infrastruktury serwerowej:**

* Serwer bazodanowy
* Macierz główna

| **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 24 godziny od czasu przyjęcia zgłoszenia | niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia |
| USTERKA | 24/7/365 | niezwłocznie, nie później niż 48 godziny od czasu przyjęcia zgłoszenia | niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia | niezwłocznie, nie później niż 5 dni od czasu przyjęcia zgłoszenia |

**Tabela 2. Usługi gwarancji dla Infrastruktury serwerowej i sieciowej:**

* Serwer wirtualizacyjny
* Serwer do kopii (backup)
* Serwer bazodanowy zapasowy
* Macierz zapasowa
* Macierz backup/serwer
* Biblioteka LTO
* Przełącznik zasobowy do macierzy
* Przełącznik zarządzający
* Przełącznik dostępowy

| **KWALIFIKACJA ZGŁOSZENIA WADY** | **OKRES DOSTĘPNOŚCI WYKONAWCY** | **ROZWIĄZANIE ZASTĘPCZE\*** | **CZAS REAKCJI WYKONAWCY** | **CZAS NAPRAWY** |
| --- | --- | --- | --- | --- |
| AWARIA | 24/7/365 | niezwłocznie nie później niż 5 dni od dnia przyjęcia zgłoszenia | niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia | niezwłocznie nie później niż 9 dni roboczych od dnia przyjęcia zgłoszenia |
| USTERKA | 24/7/365 | niezwłocznie nie później niż 9 dni roboczych od dnia przyjęcia zgłoszenia | niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia | niezwłocznie nie później niż 9 dni roboczych od dnia przyjęcia zgłoszenia |

* Przełącznik rdzeniowy (1z2)

| **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 24 godziny od czasu przyjęcia zgłoszenia | niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia |
| USTERKA | 24/7/365 | niezwłocznie, nie później niż 5 dni od czasu przyjęcia zgłoszenia | niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia | niezwłocznie, nie później niż 9 dni od czasu przyjęcia zgłoszenia |

\*nie dotyczy sprzętu zastępczego

* Przełącznik rdzeniowy (2z2)

| **KWALIFIKACJA ZGŁOSZENIA WADY** | **OKRES DOSTĘPNOŚCI WYKONAWCY** | **ROZWIĄZANIE ZASTĘPCZE\*** | **CZAS REAKCJI WYKONAWCY** | **CZAS NAPRAWY** |
| --- | --- | --- | --- | --- |
| AWARIA | 24/7/365 | niezwłocznie nie później niż 5 dni godziny od dnia przyjęcia zgłoszenia | niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia | niezwłocznie nie później niż 9 dni roboczych od dnia przyjęcia zgłoszenia |
| USTERKA | 24/7/365 | niezwłocznie nie później niż 9 dni roboczych od dnia przyjęcia zgłoszenia | niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia | niezwłocznie nie później niż 9 dni roboczych od dnia przyjęcia zgłoszenia |

\*nie dotyczy sprzętu zastępczego

**Tabela 3. Usługi gwarancji dla Infrastruktury serwerowej:**

* Szafa rack
* Zasilacz awaryjny UPS

| **KWALIFIKACJA ZGŁOSZENIA WADY** | **OKRES DOSTĘPNOŚCI WYKONAWCY** | **ROZWIĄZANIE ZASTĘPCZE\*** | **CZAS REAKCJI WYKONAWCY** | **CZAS NAPRAWY** |
| --- | --- | --- | --- | --- |
| AWARIA | W dni robocze pomiędzy godz. 8.00 a 16.00 Zgłoszenie przesłane po godz. 16.00, traktowane jest jak zgłoszenie przyjęte w następnym dniu roboczym o 8 | niezwłocznie nie później niż 5 dni robocze od dnia przyjęcia zgłoszenia | niezwłocznie nie później niż 5 dni robocze od dnia przyjęcia zgłoszenia | niezwłocznie nie później niż 10 dni roboczych od dnia przyjęcia zgłoszenia |
| USTERKA | W dni robocze pomiędzy godz. 8.00 a 16.00 Zgłoszenie przesłane po godz. 16.00, traktowane jest jak zgłoszenie przyjęte w następnym dniu roboczym o 8 | niezwłocznie nie później niż 10 dni robocze od dnia przyjęcia zgłoszenia | niezwłocznie nie później niż 10 dni robocze od dnia przyjęcia zgłoszenia | niezwłocznie nie później niż 10 dni roboczych od dnia przyjęcia zgłoszenia |

\*nie dotyczy sprzętu zastępczego

**Tabela 4. Usługi gwarancji dla oprogramowania systemowego i narzędziowego**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 24 godziny od czasu przyjęcia zgłoszenia | niezwłocznie, nie później niż 96 godziny od czasu przyjęcia zgłoszenia |
| USTERKA | W dni robocze pomiędzy godz. 8.00 a 16.00 Zgłoszenie przesłane po godz. 16.00 traktowane jest jak zgłoszenie przyjęte w następnym dniu roboczym o godz. 8.00 | nie dotyczy | niezwłocznie nie później niż 5 dni roboczych od dnia przyjęcia zgłoszenia | niezwłocznie nie później niż 30 dni roboczych od dnia przyjęcia zgłoszenia |

**Tabela 5. Usługi gwarancji dla Szpitalnego Systemu Informatycznego:**

| **KWALIFIKACJA ZGŁOSZENIA WADY** | **OKRES DOSTĘPNOŚCI WYKONAWCY** | **ROZWIĄZANIE ZASTĘPCZE** | **CZAS REAKCJI WYKONAWCY** | **CZAS NAPRAWY** |
| --- | --- | --- | --- | --- |
| AWARIA | 24/7/365 | niezwłocznie, nie później niż 12 godzin od czasu przyjęcia zgłoszenia | niezwłocznie, nie później niż 24 godzin od czasu przyjęcia zgłoszenia | niezwłocznie, nie później niż 96 godziny od czasu przyjęcia zgłoszenia |
| BŁĄD | W dni robocze pomiędzy godz.8.00 a 16.00 Zgłoszenie przesłane po godz.16.00 traktowane jest jak zgłoszenie przyjęte w następnym dniu roboczym o 8 | niezwłocznie nie później niż 14 dni roboczych od dnia przyjęcia zgłoszenia, rozwiązanie umożliwiające przekwalifikowanie na Usterkę  | niezwłocznie nie później niż 2 dni robocze od dnia przyjęcia zgłoszenia | niezwłocznie nie później niż 14 dni roboczych od dnia przyjęcia zgłoszenia |
| USTERKA | W dni robocze pomiędzy godz. 8.00 a 16.00 Zgłoszenie przesłane po godz. 16.00 traktowane jest jak zgłoszenie przyjęte w następnym dniu roboczym o godz.8.00 | nie dotyczy | niezwłocznie nie później niż 5 dni roboczych od dnia przyjęcia zgłoszenia | niezwłocznie nie później niż 30 dni roboczych od dnia 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,
6. 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. świadczenia usług w postaci konsultacji, porad, wsparcia technicznego w zakresie wdrożenia oraz użytkowania Oprogramowania, przy czym:
* usługi będą świadczone w dni robocze w godzinach od 8.00 do 16.00 w języku polskim,
* tryb zgłaszania: telefonicznie, e-mail, faxem lub poprzez System Zgłoszeń,
* 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 usługi w ciągu 3 dni roboczych, Wykonawca uzgodni z Zamawiającym inny termin konsultacji lub porady.

### 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:
		1. imię i nazwisko pracownika Wykonawcy, któremu zostanie przyznany dostęp,
		2. nazwa i adres IP zasobu (bazy danych/oprogramowania), który zostanie udostępniony,
		3. usługi sieciowe, które zostaną udostępnione,
		4. okres czasu, na który będzie aktywowany dostęp,
		5. numer zgłoszenia gwarancyjnego,
		6. przyczyna złożenia wniosku,
		7. opis czynności, które zostaną wykonane,
		8. 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 usług gwarancyjnych Wykonawca zobowiązuje się do:

* + 1. wykonywania modyfikacji bez wezwania lub na pisemne zgłoszenie Zamawiającego w celu dostosowania wszystkich elementów Oprogramowania SSI 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,
		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*,* 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;
		4. wysłania na adres korespondencyjny Zamawiającego nośnika CD/DVD zawierającego nową wersję oprogramowania, na pisemne żądanie wniesione przez Zamawiającego - każda nowa wersja musi posiadać unikalny numer;
		5. wraz z nową wersją oprogramowania Wykonawca zobowiązany jest do przekazania nowej wersji Dokumentacji wraz z procedurą instalacji oprogramowania oraz informacją o parametryzacji i konfiguracji.
		6. świadczenia usług w postaci konsultacji, porad, dodatkowej konfiguracji, tworzenia nowych raportów, wsparcia technicznego w zakresie wdrożenia oraz użytkowania oprogramowania SSI, przy czym:
* usługi 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 usługi 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 16.00 w każdym Dniu Roboczym.

W innych przypadkach należy rozumieć jako dzień kalendarzowy.