Załącznik nr 1 do SIWZ

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

DOSTAWA I WDROŻENIE INFRASTRUKTURY SERWEROWEJ I SIECIOWEJ ORAZ OPROGRAMOWANIA DLA SZPITALNEGO SYSTEMU INFORMATYCZNEGO (SSI)

Staszów 2020r.

Rozdział I. Założenia początkowe oraz wymagania ogólne

I.1 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 oraz 12 powiatowych szpitali (Samodzielnych Publicznych Zakładów Opieki Zdrowotnej).

I.2 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 eZdrowia (CeZ), 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.

I.3 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 CeZ 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 CeZ, 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 CeZ, pod adresem: http://cez.gov.pl.

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 CeZ 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 CeZ.
- 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/lub 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 CeZ.

- W przypadku rejestru (indeksu) Elektronicznej Dokumentacji Medycznej – obowiązuje EDMiZM publikowany przez CeZ.
- 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 CeZ.
- 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 CeZ.

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

- Prowadzenie i wymiana Elektronicznej Dokumentacji Medycznej (EDM), w tym indywidualnej dokumentacji medycznej (wewnętrznej lub 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 CeZ – 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.
- Szpitalny System Informatyczny powinien być zintegrowany z systemem zrealizowanym w ramach projektu „Tryby Obsługi Pacjenta w Szpitalnym Oddziale Ratunkowym (TOPSOR)" współfinansowanym ze środków Unii Europejskiej w ramach Programu Operacyjnego Infrastruktura i Środowisko 2014-2020".

I.4 Akty prawne

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

I.5 Ogólny opis przedmiot zamówienia

Dostawa i wdrożenie infrastruktury serwerowej oraz oprogramowania dla Szpitalnego Systemu Informatycznego (SSI).

Przedmiot zamówienia niniejszego postępowania przetargowego obejmuje:

1) **dostawę i wdrożenie Infrastruktury Serwerowej wraz z oprogramowaniem systemowym i narzędziowym:**

- **Infrastruktura serwerowa i sprzęt komputerowy** w zakresie:

POZ. SOPZ	OPIS	ILOŚĆ SZTUK
ROZDZIAŁ II.1	**INFRASTRUKTURA SERWEROWA**	
II.1.1	Serwer wirtualizacyjny	2
II.1.2	Serwer do kopii (backup)	1
II.1.3	Serwer bazodanowy	2
II.1.4	Macierz główna	1
II.1.5	Biblioteka LTO	1
II.1.6	Przełącznik zasobowy do macierzy	2
II.1.7	Zasilacz awaryjny UPS	1
II.1.8	Szafa Rack	1
II.3.5	Infokiosk z wbudowaną drukarką	2
II.3.5	Wyświetlacz gabinetowy 21”	20
II.3.5	Wyświetlacz rejestracja 21”	5
II.3.5	Wyświetlacz duży zbiorczy 50’’	1
II.3.5	Drukarka biletów	1
II.1.9	Przełącznik LAN	1
II.1.10	Przełącznik zarządzający	1
II.1.11	Punk dostępowy wewnętrzny	6
II.1.12	UTM	1

- **Oprogramowanie systemowe i narzędziowe** w zakresie:

POZ. SOPZ	OPIS	ILOŚĆ
ROZDZIAŁ II.2	**OPROGRAMOWANIE SYSTEMOWE I NARZĘDZIOWE**	
II.2.1	Oprogramowanie systemowe – SSO, wirtualizacja i CAL	1 kpl.:
	Oprogramowanie 1- systemy operacyjne dla serwerów	1 kpl. dla 3 fizycznych serwerów

	Oprogramowanie 2- licencje dostępowe do systemów operacyjnych oprogramowania systemowego	80 szt.
II.2.2	Oprogramowanie do robienia kopii zapasowych	1

2) dostawę i wdrożenie oprogramowania dla Szpitalnego Systemu Informatycznego SSI:

POZ. SOPZ	OPIS
ROZDZIAŁ II.3	**SZPITALNY SYSTEM INFORMATYCZNY**
II.3.5	HIS - moduły – część medyczna – dostawa i wdrożenie
	e-Usługi – dostawa i wdrożenie
II.3.5	Elektroniczna Dokumentacja Medyczna – dostawa i wdrożenie
II.3.8	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 oraz wdrożenia.

3. 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.
4. Wykonawca jest zobowiązany do realizacji Przedmiotu Zamówienia zgodnie z zasadami i wytycznymi Zamawiającego, zapisami SOPZ oraz Umowy.
5. 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 załączniku 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.

6. Wykonawca musi dostarczyć wszelkie urządzenia, elementy, oprogramowanie, które są niezbędne do prawidłowego funkcjonowania całości. W przypadku, gdy w trakcie realizacji Przedmiotu Zamówienia okaże się, że brakuje jakiegokolwiek urządzenia, elementu, licencji oprogramowania, którego brak spowoduje nieprawidłowe funkcjonowanie całości Przedmiotu Zamówienia, Wykonawca dostarczy je na własny koszt.
7. 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.
8. 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 żadnym modyfikacjom.
- Wszystkie dostarczane urządzenia muszą być wyprodukowane po dniu 1 stycznia 2020r.

I.6 Termin realizacji Przedmiotu Zamówienia

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

I.7 Organizacja wdrożenia

I.7.1 Założenia podstawowe

1. Przedmiot Zamówienia będzie realizowany w oparciu o zdefiniowany uprzednio przez Wykonawcę i zaakceptowany Harmonogram wdrożenia, który powinien być uzgodniony i zaakceptowany przez Zamawiającego oraz odpowiednio utrzymywany w toku realizacji Przedmiotu Zamówienia.
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 musi być ona oznakowana w taki sposób, aby możliwa była identyfikacja systemowa zarówno produktu jak i producenta, pochodzić z oficjalnych kanałów dystrybucji producentów i dostarczony w oryginalnych opakowaniach fabrycznych.
7. Wdrożenie należy rozumieć jako szereg uporządkowanych i zorganizowanych działań mających na celu wykonanie Przedmiotu Zamówienia.
8. Wdrożenie będą 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:
    a. Koordynator Projektu ze strony Wykonawcy,

b. Zespół Wdrożeniowy ze strony Wykonawcy

10. Wdrożenie, z zastrzeżeniami wskazanymi poniżej, w punktach muszą realizować osoby wymienione w ofercie Wykonawcy, przy czym:
    a. Osoby Zespołu Wykonawcy muszą być dyspozycyjne w trakcie wykonywania prac,
    b. Wykonawca przekaże Zamawiającemu wykaz numerów telefonów kontaktowych do 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.

I.7.2 Przygotowanie Dokumentacji

1. W ramach procesu prac Wykonawca opracuje dla Zamawiającego Dokumentację Przedmiotu Zamówienia (zwaną dalej Dokumentacją), która składa się z nw. zakresów:

a) Harmonogram Wdrożenia.
b) Dokumentacja Analizy Przedwdrożeniowej (DAP).
c) Dokumentacja Powykonawcza.

2. 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.

3. Dokumentacja podlega uzgadnianiu i akceptacji Zamawiającego. Akceptacja Harmonogramu wdrożenia oraz DAP warunkuje rozpoczęcie prac Wykonawcy.
4. Dokumentacja Analizy Przedwdrożeniowej DAP wraz z Harmonogramem wdrożenia zostaną opracowane w oparciu o wymagania określone w niniejszym SOPZ.

I.7.3 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.

I.7.4 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:

SKŁAD DAP
SSI
– wykaz oraz szczegółowy opis i harmonogram wdrożenia SSI lub/i e-usług
– architekturę SSI i e-usług
– analizę i plan migracji danych oraz opis sposobu migracji danych z SSI, który posiada Zamawiający – jeżeli dotyczy
– przygotowanie planu instalacji Infrastruktury serwerowej
– przygotowanie planu instalacji macierzy dyskowych
– jednoznacznie określone założenia integracji z innymi systemami informatycznymi, które posiada Zamawiający
– plan pracy na wszystkie etapy Wdrożenia
– 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 - jeżeli dotyczy
– lista Komponentów, które będę podlegały osobnym odbiorom – jeżeli dotyczy
– szczegółowy zakres i zawartość pozostałej Dokumentacji
DOKUMENTACJA POWYKONAWCZA LOGICZNEJ STRUKTURY SIECI
– Informacje ogólne
– Opis sposobu i struktury adresacji logicznej sieci
– Ogólny schemat logicznej struktury sieci

I.7.5 Dokumentacja Powykonawcza

1. Warunkiem dokonania Odbioru Końcowego jest dostarczenie przez Wykonawcę Dokumentacji Powykonawczej obejmującej dokumentację użytkową, techniczną i eksploatacyjną. Dokumentacja Powykonawcza musi być dostarczona w języku polskim, w wersji elektronicznej w formacie edytowalnym oraz w co najmniej jednym egzemplarzu papierowym.
2. W dokumentacji muszą być zawarte opisy wszelkich cech, właściwości i funkcjonalności pozwalających na poprawną z punktu widzenia technicznego eksploatację rozwiązań.
3. W szczególności dokumentacja ta powinna zawierać następujące elementy:

Wymogi ogólne:

1. Pełna charakterystyka i opis sposobu licencjonowania elementów aplikacji i środowiska.
2. Opis architektury technicznej:
    - wyszczególnienie oraz opis minimalnych wymagań sprzętowych, systemowych i aplikacyjnych wymaganych do poprawnej pracy aplikacji zgodnie z wymaganiami wydajności, funkcjonalności i bezpieczeństwa.
    - Objaśnienie wykonanej konfiguracji wdrożonego systemu oraz urządzeń, zainstalowanych w ramach budowy systemu IT.
    - Opis architektury logicznej systemu.
    - Opis zainstalowanej bazy danych.
3. Dokumentacja administracyjna związana z poprawną eksploatacją

a. opis (w postaci procedur lub instrukcji) wszystkich rutynowych czynności administracyjnych dla aplikacji i systemu informatycznego (dziennych, tygodniowych, miesięcznych itp.),
b. opis 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.),
c. opis zalecanego trybu backupu aplikacji i elementów infrastruktury software'owej, oraz zakres danych podlegających backupowi.

4. Dokumenty z testów:
   a. plan testów, opis realizacji testów akceptacyjnych funkcjonalności wybranych przez Zamawiającego i Wykonawcę.
5. Dokumentacja wdrożeniowa:
   a. dokumentacja powdrożeniowa: zawiera opis wykonanych czynności instalacyjnych oraz konfiguracyjnych wszystkich komponentów systemu.
   b. Instrukcje obsługi i instrukcje użytkowania dla wersji dostarczonego oprogramowania z podziałem na poszczególne moduły.
   c. W zakresie obszarów administratora dokumentacja powinna zawierać dodatkowo co najmniej:

- opis podstawowych ról użytkowników,
- opis zarządzania uprawnieniami użytkownika.
- Opis sposobu przetwarzania danych oraz wykaz zbiorów danych osobowych.

I.7.6 Odbiór

1. Odbiór 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>

I.7.7 Dostawa i instalacja oprogramowania standardowego

1. Oprogramowanie standardowe rozumiane jako oprogramowanie dostarczone i zainstalowane na Infrastrukturze serwerowej oraz sieciowej posiadanej przez Zamawiającego i/lub dostarczanej 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. Oprogramowanie standardowe musi zostać skonfigurowane tak, aby działało poprawnie zgodnie z jego przeznaczeniem i architekturą Systemu oraz zapewniało prawidłową pracę Oprogramowania aplikacyjnego.

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

1. Zadanie dostawy, instalacji, konfiguracji i wdrożenia Oprogramowania aplikacyjnego obejmuje:
   a) SSI (HIS) wraz z migracją bazy danych do wydajnego silnika bazodanowego,
   b) EDM,
   c) E-usługi.
2. Dostawa i instalacja muszą być wykonane w lokalizacji 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 procesu wdrażania z oczekiwaniami konfiguracyjnymi (w zakresie opisanych w OPZ wymagań funkcjonalnych).
4. Oprogramowanie aplikacyjne musi zostać zainstalowane przez Wykonawcę w szczególności z wykorzystaniem Sprzętu dostarczanego przez Wykonawcę i w środowiskach informatycznych Zamawiającego. Oprogramowanie aplikacyjne musi zostać zainstalowane i skonfigurowane w sposób kompleksowy na wszystkich stanowiskach komputerowych Zamawiającego.
5. Zamawiający na potrzeby realizacji przedmiotu zamówienia przewidział infrastrukturę serwerową i oprogramowanie o parametrach wskazanych w rozdziale II niniejszego SOPZ.

I.7.9 Testy

1. W ramach postepowania 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 lub 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. Zamawiający w końcowej fazie wdrożenia oczekuje realizacji przez Wykonawcę testów bezpieczeństwa.
5. Testy te będą prowadzone w środowisku produkcyjnym systemu teleinformatycznego w co najmniej 2 iteracjach.
6. W przypadku zidentyfikowania Błędów lub Wad Wykonawca jest zobowiązany do ich poprawy przed odbiorem Końcowym Przedmiotu Zamówienia.

I.7.10 Dodatkowe zobowiązania Wykonawcy

1. Wykonanie Przedmiotu Zamówienia z efektywnością oraz zgodnie z praktyką i wiedzą zawodową.
2. 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.

Rozdział II. Szczegółowy opis przedmiotu zamówienia

II.1 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 dostarczoną Infrastrukturą Serwerową, Wykonawca zobowiązany jest dostarczyć niezbędne elementy np. urządzenia i wyposażenie – kable połączeniowe, elementy mocujące, uznane przez Wykonawcę za niezbędne i umożliwiające prawidłowe działanie całego Systemu. Dostarczona Infrastruktura Serwerowa musi zapewniać bezproblemową pracę po podłączeniu jej do sieci informatycznej Zamawiającego.
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 szafie serwerowej rack, w sposób umożliwiający ich prawidłową wentylację.
5. Szczegóły dotyczące instalacji i uruchomienia Infrastruktury serwerowej zostaną ustalone w trakcie Analizy Przedwdrożeniowej.
6. 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
  - Propozycję testów odbiorczych
  - ➢ Instalacja, montaż i uruchomienie serwerów wirtualizacyjnych:
  - Montaż serwera w istniejącej szafie rackowej
  - 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
- 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

7. Po zakończonym montażu Wykonawca przekaże Zamawiającemu wszystkie hasła dostępowe do kont „super użytkowników” oraz dokumentację do wszystkich oferowanych urządzeń, oprogramowania narzędziowego (systemowego, bazodanowego, wirtualizacyjnego, backupowego itd.) wraz z dokumentami potwierdzającymi nabycie dla Zamawiającego licencji oraz nośnikami danych zawierającymi zainstalowane oprogramowanie. Wykonawca wykona również instruktaże użytkowe dla wskazanego przez Zamawiającego administratora, z zakresu konfiguracji, obsługi i prawidłowej eksploatacji zainstalowanego Sprzętu ze szczególnym uwzględnieniem obsługi i zaawansowanego zarządzania macierzą danych w środowisku Zamawiającego.

8. Wykonawca zobowiązany jest zapewnić 6 miesięczne wsparcie i możliwość prowadzenia konsultacji w zakresie administracji zaoferowanym sprzętem oraz dostarczonym oprogramowaniem narzędziowym (systemowym, wirtualizacyjnym, backup-owym i bazodanowym) w ilości nie większej niż 30 godzin.

II.1.1 Serwer wirtualizacyjny

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

CECHA	WYMAGANIA MINIMALNE
Obudowa	Maksymalnie 1U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia) Serwer posiadający możliwość zamontowania zamykanego, zdejmowanego panelu przedniego chroniącego przed nieuprawionym dostępem do dysków Serwer posiadający możliwość zamontowania czujnika otwarcia obudowy współpracującego z BIOS.
Procesor	Procesor ośmiordzeniowy, x86 - 64 bity, taktowanie min. 2.1GHz, pamięć cache min. 11MB, osiągający w testach PassMark – CPU Mark wynik nie gorszy niż 11000 punktów. Wynik testu musi być opublikowany na stronie www.cpubenchmark.net **Zamawiający zweryfikuje wydajność zaoferowanego procesora według wyników testów procesorów opublikowanych na stronie: www.cpubenchmark.net w dniu ogłoszenia zamówienia na stronie Zamawiającego.** Płyta główna wspierająca zastosowanie dwóch procesorów od 4 do 28 rdzeniowych, mocy do min. 205W i taktowaniu CPU do min. 3.6GHz.
Liczba procesorów	Min. 2 procesory
Pamięć operacyjna	Minimum 128 GB RDIMM DDR4 2666 MT/s w identycznych modułach o pojemności min. 32GB każdy, przy czym ilość modułów i pamięci w serwerze musi być taka sama dla każdego z procesorów. Płyta główna z minimum 24 slotami na pamięć i umożliwiająca instalację do minimum 6TB. Płyta główna z fabrycznym oznaczeniem logo producenta (dopuszcza się logo producenta na module zarządzania trwale zintegrowanym na płycie głównej).

	Obsługa zabezpieczeń: Advanced ECC i Online Spare. Serwer z obsługą pamięci typu NVDIMM i Intel Optane (128GB, 256GB, 512GB).
Sloty rozszerzeń	2 aktywne gniazda PCI-Express generacji 3, w tym min. 1 slot x16 (prędkość slotu – bus width) pełnej wysokości (full height). Możliwość rozbudowy o dodatkowy, trzeci slot PCI-Express generacji 3 x16 (prędkość slotu – bus width). Po instalacji wszystkich wymaganych kart rozszerzeń, serwer musi mieć możliwość rozbudowy o dodatkową kartę rozszerzeń w gnieździe PCI-Express.
Dysk twardy	Zatoki dyskowe gotowe do zainstalowania 8 dysków SFF typu Hot Swap SAS/SATA/SSD 2,5” i opcja rozbudowy/rekonfiguracji o dodatkowe 2 dyski typu Hot Swap SAS/SATA/SSD. Zainstalowane minimum 2 dyski typu SAS 12G o pojemności minimum 300 GB każdy.
Kontroler	Serwer wyposażony w kontroler sprzętowy z min. 2GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę 8 napędów dyskowych SAS oraz obsługujący poziomy: RAID 0/1/10/5/50/6/60. Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie Serwer umożliwiający rozbudowę o sprzętowy kontroler RAID zapewniający obsługę RAID 0/1/10/5/50/6/60 z 4GB pamięci cache z podtrzymywaniem bateryjnym.
Interfejsy sieciowe	Min. 4 porty Ethernet 100/1000 Mb/s Base-T z funkcją Wake-On-LAN, wsparciem dla PXE, które nie zajmują gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”. Dwie 2-portowe karty sieciowe Ethernet 10 Gb/s SFP+ (łącznie minimum 4 porty 10 Gb/s SFP+).
Karta graficzna	Zintegrowana karta graficzna
Porty	4 x USB (w tym min. 2 USB 3.0 i 1 port USB wewnętrzny) 1x VGA Możliwość rozbudowy o: - port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45
Pamięć flash	Serwer umożliwiający instalację pamięci flash w postaci kart microSD/SD zapewniających minimalną pojemność 8GB.

Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 500W.
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug Możliwość skonfigurowania serwera do pracy w temperaturze otoczenia równej 45st.C, tak, żeby zapewnić zgodność ze standardem ASHRAE Class A4
Napęd	Możliwość instalacji wewnętrznego napędu DVD-ROM lub DVD-RW
Karta/moduł zarządzający	Niezależna od systemu operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski (fizyczne i logiczne), karty sieciowe • wparcie dla agentów zarządzających oraz możliwość pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez - dedykowany port RJ45 z tyłu serwera - przez współdzielony port zintegrowanej karty sieciowej serwera dostęp do karty możliwy - z poziomu przeglądarki webowej (GUI) - z poziomu linii komend; - z poziomu skryptu (XML/Perl) - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) • wbudowane narzędzia diagnostyczne • zdalna konfiguracja serwera (BIOS) i instalacji systemu operacyjnego • obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie • wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników • przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP

	passthrough) • obsługa zdalnego serwera logów (remote syslog) • wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i wirtualnych folderów • mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie • funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji • konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) • zdalna aktualizacja oprogramowania (firmware) • zarządzanie grupami serwerów, w tym: - tworzenie i konfiguracja grup serwerów - sterowanie zasilaniem (wł/wył) - ograniczenie poboru mocy dla grupy (power caping) - aktualizacja oprogramowania (firmware) - wspólne wirtualne media dla grupy • możliwość równoczesnej obsługi przez 6 administratorów • wsparcie dla Microsoft Active Directory • obsługa SSL i SSH • enkrypcja AES/3DES • wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Microsoft Windows Server 2012 R2, 2016, 2019 Red Hat Enterprise Linux (RHEL) 7.x oraz 8.x SUSE Linux Enterprise Server (SLES) 12 oraz 15 CentOS VMware ESXi 6.0, 6.5, 6.7, 7

II.1.2 Serwery do kopii (backup)

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

CECHA	WYMAGANIA MINIMALNE
Obudowa	Maksymalnie 2U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia)
Procesor	Procesor ośmiordzeniowy, x86 - 64 bity, taktowanie min. 2.1GHz, pamięć cache min. 11MB, osiągający w testach PassMark – CPU Mark wynik nie gorszy niż 11000 punktów. Wynik testu musi być opublikowany na stronie www.cpubenchmark.net. **Zamawiający zweryfikuje wydajność zaoferowanego procesora według wyników testów procesorów opublikowanych na stronie: www.cpubenchmark.net w dniu ogłoszenia o zamówienia na stronie Zamawiającego.** Płyta główna wspierająca zastosowanie dwóch procesorów od 4 do 28 rdzeniowych, mocy do min. 205W i taktowaniu CPU do min. 3.6GHz.
Liczba procesorów	Min. 1 procesor
Pamięć operacyjna	Minimum 32 GB RDIMM DDR4 2666 MT/s w modułach o pojemności 16GB każdy. Płyta główna z minimum 24 slotami na pamięć i umożliwiająca instalację do minimum 6TB. Płyta główna z fabrycznym oznaczeniem logo producenta (dopuszcza się logo producenta na module zarządzania trwale zintegrowanym na płycie głównej). Obsługa zabezpieczeń: Advanced ECC i Online Spare. Serwer z obsługą pamięci typu NVDIMM i Intel Optane (128GB, 256GB, 512GB).
Sloty rozszerzeń	3 aktywne gniazda PCI-Express generacji 3, gotowe do obsadzenia kartami rozszerzeń, w tym min. 1 slot x16 (szybkość slotu – bus width) pełnej wysokości (full height). Możliwość rozbudowy o 5 dodatkowych slotów PCI-Express generacji 3, w tym minimum 1 slot x16 (szybkość slotu – bus width)
Dysk twardy	Zatoki dyskowe gotowe do zainstalowania 12 dysków LFF typu Hot Swap, SAS/SATA/SSD, 3,5” i opcja rozbudowy/rekonfiguracji serwera o dodatkowe 4

	dyski typu Hot Swap, SAS/SATA/SSD. Zainstalowane minimum 8 dysków SATA 6G LFF o pojemności minimum 8 TB każdy oraz minimum 2 dyski SSD SATA 6G Mixed Use o pojemności 960 GB każdy, posiadające współczynnik DWPD nie gorszy niż 3,0.
Kontroler	Serwer wyposażony w kontroler sprzętowy z min. 4GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę 16 napędów dyskowych SAS oraz obsługujący poziomy: RAID 0/1/10/5/50/6/60. Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie
Dodatkowy kontroler	Serwer wyposażony w kontroler sprzętowy SAS 12 Gb/s z minimum dwoma portami zewnętrznymi SAS x4, do podłączenia autoloadera z napędem taśmowym SAS.
Interfejsy sieciowe	Minimum 4 porty Ethernet 100/1000 Mb/s Base-T z funkcją Wake-On-LAN, wsparciem dla PXE, które nie zajmują gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”. Minimum 2 porty Ethernet 10 Gb/s SFP+
Karta graficzna	Zintegrowana karta graficzna
Porty	3 x USB (w tym min. 2 USB 3.0 i 1 port USB wewnętrzny) 1 x VGA Możliwość rozbudowy o: - port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45
Pamięć flash	Serwer umożliwiający instalację pamięci flash w postaci kart microSD/SD zapewniających minimalną pojemność 8GB.
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 800W.
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
Karta/moduł zarządzający	Niezależna od systemu operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski (fizyczne i logiczne), karty sieciowe • wparcie dla agentów zarządzających oraz możliwość pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie

	operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez - dedykowany port RJ45 z tyłu serwera lub - przez współdzielony port zintegrowanej karty sieciowej serwera dostęp do karty możliwy - z poziomu przeglądarki webowej (GUI) - z poziomu linii komend; - z poziomu skryptu (XML/Perl) - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) • wbudowane narzędzia diagnostyczne • zdalna konfiguracja serwera (BIOS) i instalacji systemu operacyjnego • obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie • wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników • przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough) • obsługa zdalnego serwera logów (remote syslog) • wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i wirtualnych folderów • mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie • funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji • konfiguracja maksymalnego poziomu pobieranej mocy przez serwer

	(capping) • zdalna aktualizacja oprogramowania (firmware) • zarządzanie grupami serwerów, w tym: - tworzenie i konfiguracja grup serwerów - sterowanie zasilaniem (wł/wył) - ograniczenie poboru mocy dla grupy (power caping) - aktualizacja oprogramowania (firmware) - wspólne wirtualne media dla grupy • możliwość równoczesnej obsługi przez 6 administratorów • wsparcie dla Microsoft Active Directory • obsługa SSL i SSH • enkrypcja AES/3DES • wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Microsoft Windows Server 2012 R2, 2016, 2019 Red Hat Enterprise Linux (RHEL) 7.x oraz 8.x SUSE Linux Enterprise Server (SLES) 12 oraz 15 CentOS VMware ESXi 6.0, 6.5, 6.7, 7

II.1.3 Serwer bazodanowy

Wymagane jest dostarczenie 2 szt. Serwera spełniającego poniżej opisane minimalne parametry funkcjonalne:

CECHA	WYMAGANIA MINIMALNE
Obudowa	Maksymalnie 1U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia) Serwer posiadający możliwość zamontowania zamykanego, zdejmowanego panelu przedniego chroniącego przed nieuprawionym dostępem do dysków Serwer posiadający możliwość zamontowania czujnika otwarcia obudowy współpracującego z BIOS.
Procesor	Procesor ośmiordzeniowy, x86 - 64 bity, taktowanie min. 3.0 GHz, pamięć cache min. 11MB, osiągający w testach PassMark – CPU Mark wynik nie gorszy

	niż 14000 punktów lub **wynik dla procesora w konfiguracji „Dual CPU". W przypadku występowania procesora na liście www.cpubenchmark.net tylko w konfiguracji „Dual CPU", oferowany procesor musi osiągać wynik min. 24000 punktów.** Wynik testu musi być opublikowany na stronie www.cpubenchmark.net. **Zamawiający zweryfikuje wydajność zaoferowanego procesora według wyników testów procesorów opublikowanych na stronie: www.cpubenchmark.net w dniu ogłoszenia o zamówienia na stronie Zamawiającego.** Płyta główna wspierająca zastosowanie dwóch procesorów od 4 do 28 rdzeniowych, mocy do min. 205W i taktowaniu CPU do min. 3.6GHz.
Liczba procesorów	Min. 1 procesor
Pamięć operacyjna	Minimum 128 GB RDIMM DDR4 2666 MT/s w identycznych modułach o pojemności min. 32GB każdy, przy czym ilość modułów i pamięci w serwerze musi być taka sama dla każdego z procesorów. Płyta główna z minimum 24 slotami na pamięć i umożliwiająca instalację do minimum 6TB. Płyta główna z fabrycznym oznaczeniem logo producenta (dopuszcza się logo producenta na module zarządzania trwale zintegrowanym na płycie głównej). Obsługa zabezpieczeń: Advanced ECC i Online Spare. Serwer z obsługą pamięci typu NVDIMM i Intel Optane (128GB, 256GB, 512GB).
Sloty rozszerzeń	2 aktywne gniazda PCI-Express generacji 3, w tym min. 1 slot x16 (prędkość slotu – bus width) pełnej wysokości (full height). Możliwość rozbudowy o dodatkowy, trzeci slot PCI-Express generacji 3 x16 (prędkość slotu – bus width). Po instalacji wszystkich wymaganych kart rozszerzeń, serwer musi mieć możliwość rozbudowy o dodatkową kartę rozszerzeń w gnieździe PCI-Express.
Dysk twardy	Zatoki dyskowe gotowe do zainstalowania 8 dysków SFF typu Hot Swap SAS/SATA/SSD 2,5" i opcja rozbudowy/rekonfiguracji o dodatkowe 2 dyski typu Hot Swap SAS/SATA/SSD. Zainstalowane minimum 2 dyski typu SAS 12G o pojemności minimum 300 GB każdy.
Kontroler	Serwer wyposażony w kontroler sprzętowy z min. 2GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę 8 napędów dyskowych SAS oraz obsługujący poziomy:

	RAID 0/1/10/5/50/6/60. Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie Serwer umożliwiający rozbudowę o sprzętowy kontroler RAID zapewniający obsługę RAID 0/1/10/5/50/6/60 z 4GB pamięci cache z podtrzymywaniem bateryjnym.
Interfejsy sieciowe	Min. 4 porty Ethernet 100/1000 Mb/s Base-T z funkcją Wake-On-LAN, wsparciem dla PXE, które nie zajmują gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”. Dwie 2-portowe karty sieciowe Ethernet 10 Gb/s SFP+ (łącznie minimum 4 porty 10 Gb/s SFP+)
Karta graficzna	Zintegrowana karta graficzna
Porty	4 x USB (w tym min. 2 USB 3.0 i 1 port USB wewnętrzny) 1x VGA Możliwość rozbudowy o: - port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45
Pamięć flash	Serwer umożliwiający instalację pamięci flash w postaci kart microSD/SD zapewniających minimalną pojemność 8GB.
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 500W.
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug Możliwość skonfigurowania serwera do pracy w temperaturze otoczenia równej 45st.C, tak, żeby zapewnić zgodność ze standardem ASHRAE Class A4
Napęd	Możliwość instalacji wewnętrznego napędu DVD-ROM lub DVD-RW
Karta/moduł zarządzający	Niezależna od systemu operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski (fizyczne i logiczne), karty sieciowe • wparcie dla agentów zarządzających oraz możliwość pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez - dedykowany port RJ45 z tyłu serwera

	- przez współdzielony port zintegrowanej karty sieciowej serwera dostęp do karty możliwy - z poziomu przeglądarki webowej (GUI) - z poziomu linii komend; - z poziomu skryptu (XML/Perl) - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) • wbudowane narzędzia diagnostyczne • zdalna konfiguracja serwera (BIOS) i instalacji systemu operacyjnego • obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie • wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników • przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough) • obsługa zdalnego serwera logów (remote syslog) • wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i wirtualnych folderów • mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie • funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji • konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) • zdalna aktualizacja oprogramowania (firmware) • zarządzanie grupami serwerów, w tym:

	- tworzenie i konfiguracja grup serwerów - sterowanie zasilaniem (wł/wył) - ograniczenie poboru mocy dla grupy (power caping) - aktualizacja oprogramowania (firmware) - wspólne wirtualne media dla grupy • możliwość równoczesnej obsługi przez 6 administratorów • wsparcie dla Microsoft Active Directory • obsługa SSL i SSH • enkrypcja AES/3DES • wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	– Microsoft Windows Server 2012 R2, 2016, 2019 – Red Hat Enterprise Linux (RHEL) 7.x oraz 8.x – SUSE Linux Enterprise Server (SLES) 12 oraz 15 – CentOS – VMware ESXi 6.0, 6.5, 6.7, 7

II.1.4 Macierz główna

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

CECHA	WYMAGANIA MINIMALNE
Opis urządzenia	Oferowane urządzenie jest zoptymalizowaną pod kątem flash hybrydową pamięcią dyskową z dostępem przez interfejsy 10GbE/16Gb FC oraz wewnętrzną magistralą 12Gbps. Przez macierz dyskową Zamawiający rozumie zestaw nośników do składowania danych obsługiwanych przez dedykowane kontrolery macierzowe (bez dodatkowych urządzeń pośrednich, serwerów wirtualizujących, oprogramowania wirtualizującego itp.). Spełnienie wymagań poniżej powinno być udokumentowane w ogólnodostępnych materiałach producenta.

Wsparcie klastrów i systemów operacyjnych	Urządzenie musi być na listach wsparcia i wspierać główne systemy operacyjne i klastry, w tym: system operacyjny Windows Server 2012, Windows Server 2016, Windows Server 2019, VMware 7, Linux (Centos 7.x, SUSE12, Redhat 7.x). Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Preferowane jest rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. W przypadku stosowania rozwiązań firmowych/własnych – konieczna jest ich certyfikacja dla platform: Windows 2012+, Linux RedHat 7.x+, Suse12+, VMware 5,5+, oraz stosowanego oprogramowania w tym SAP(HANA) itp. Wsparcie dla wymienionych systemów operacyjnych i klastrowych musi być potwierdzone wpisem na ogólnodostępnej liście kompatybilności producentów. Jeżeli dla realizacji powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów/pojemności obsługiwanych przez oferowane urządzenie.
Pojemność i skalowalność	Oferowane Urządzenie musi być wyposażone w: a) Surową pojemność zbudowaną z $(1+W_1+W_2+W_3)*21$ nośników/dysków. b) Pojemność netto $(1+W_3)*14,8$TiB (po odjęciu narzutu na RAID, przestrzeni/dysków hotspare oraz metadanych) c) Dedykowaną pamięcią podręczną flash zbudowaną z dysków SSD o pojemności użytecznej $(1+W_5)*1,3$TiB zbudowaną z minimum 6 dysków SSD. zapewniać rozbudowę: d) W trybie scale-up do $(1+W_1+W_2)*147$ nośników danych o łącznej przestrzeni surowej 1260TB przez rozbudowę kontrolerów i dodanie dysków/półek dyskowych. e) scale-out do 5PB przestrzeni surowej przez integrację do 8 kontrolerów w sposób zapewniający stworzenie pojedynczej, jednolitej puli dyskowej dla świadczonych serwisów z wykorzystaniem wbudowanego w macierz oprogramowania klastrowego. Używane jednostki pojemności: $1TiB=1024GiB=2^{40}B$, $1GiB=1024MiB=2^{30}B$

	1TB=1000GB=10^{12}B, 1GB=1000MB=10^{6}B
Bufor danych RAM	Każdy kontroler oferowanego Urządzenia musi być wyposażony w (1+W_6)*32GB pamięci RAM dedykowanej dla operacji odczytu i zapisu z zastrzeżeniem: a) Wyszczególniona pojemność musi być dedykowana na dane i informacje kontrolne. FW/OS musi posiadać własną dedykowaną pamięcią operacyjną różną od wyspecyfikowanej powyżej. b) Pamięć zapisów musi być zabezpieczona dodatkową kopią zabezpieczającą przed awarią kontrolera i utratą zasilania. Rozbudowa opisana w części „Pojemność i skalowalność" musi pozwalać na zwiększenie RAM kontrolera do (1+W_6)*128GB
Efektywność obsługi nośników danych	Dla urządzenia zapewniającego grupowanie i sekwencyjny zrzut zdeduplikowanych i skompresowanych danych z bufora podręcznego na wewnętrzne nośniki danych sekwencyjnie, pakietem nie mniejszym niż 8MB współczynnik W_2=0. Inne rozwiązania W_2=3.
Bufor Flash	a) Oferowane urządzenie musi zapewniać możliwość rozbudowy wielkości buforu flash do pojemności (1+W_5)*28TB netto dynamicznie (zwiększanie i zmniejszanie) w oferowanej konfiguracji. b) Współczynnik W_5=0 można zastosować dla urządzeń przechowywujących w buforze flash zdeduplikowane i skompresowane dane. W pozostałych przypadkach W_5=2 c) Oferowane rozwiązanie musi zapewniać równoczesny zrzut zdeduplikowanych i skompresowanych **danych** na dyski oraz do bufora flash. Dane w buforze muszą być dobierane na podstawie tzw. „heat map" (częstotliwości używania obszaru) W_6=0 w przeciwnym razie W_6=2 Termin deduplikacja i kompresja odnosi się do urządzeń zapewniających deduplikację z granulacją 4kB oraz kompresję algorytmem lze realizowanymi w locie (inline), to jest przed zapisem na dyski/nośniki danych. Zamawiający dopuszcza, aby urządzenie, w celu zapewnienia wymaganej wydajności, dynamicznie redukowało algorytm kompresji na nie gorszy niż lz4 dla obciążeń kontrolerów powyżej 70% pod warunkiem, że kompresja zawsze odbywa się w locie (inline).
Brak pojedynczego punktu	Oferowane urządzenie musi być wolne od Pojedynczych Punktów Awarii,

awarii	czyli wszystkie komponenty: kontrolery, bufor flash, wentylatory, zasilacze itp. muszą być redundantne. Awaria pojedynczego komponentu w tym kontrolera nie może powodować spadku wydajności urządzenia poniżej parametrów granicznych.
Wsparcie dysków i szyfrowania	Oferowane urządzenie musi wspierać dyski SSD o pojemnościach 240 ,480, 960, 1920, 3840GB na potrzeby bufora danych oraz dyski 1, 2, 4, 6, 10TB dla przechowywania danych. Oferowane urządzenie musi wspierać certyfikowane szyfrowanie zgodne z AES-256 XTS FIPS z granulacją i dedykowanym kluczem dla każdego prezentowanego LUN.
Woluminy: wspierana ilość i zabezpieczenie RAID	Macierz (W_3=0) musi: a) zabezpieczać przed jednoczesną utratą 2 dysków bez utraty danych. b) zapewnić przestrzeń hot spare w wymiarze 1 dysk na każde 24 dyski. c) udostępniać jednolitą, pojedynczą pulę złożoną ze wszystkich dysków na potrzeby tworzenia woluminów danych. d) wspierać udostępnianie nie mniej niż 1024 woluminów (LUN). Zamawiający dopuszcza Macierze wymagające dedykowanych pul dla migawek lub zabezpieczonych RAID6, w takim przypadku należy zastosować współczynnik ekwiwalentności W_3=0,5.
Dostępność	a) Rozwiązanie ma charakteryzować się udokumentowaną dostępnością 99,999%. b) Być wolne od pojedynczych punktów awarii. c) Zapewnić wydajność 21 000 IOps dla obciążenia typu losowego, blokiem 4kB przy stosunku odczytów do zapisów 50/50 (dla oferowanej konfiguracji) w: i. przypadku awarii (niedostępności) jednego kontrolera ii. trakcie procesów aktualizacji oprogramowania i poprawek kontrolerów, sterowników/firmware'u iii. przy zabezpieczeniu RAID Wydajność musi być potwierdzona wydrukiem z „sizera" producenta dla oferowanej konfiguracji sprzętowej. Zamawiający zastrzega sobie prawo do zażądania od oferenta przeprowadzenia testów wydajnościowych z wykorzystaniem narzędzia iorate lub iometer na analogicznej do proponowanej konfiguracji sprzętowej.
Raportowanie i zalecenia	Macierz musi umożliwiać generowanie raportów dla kierownictwa w

dla kierownictwa	minimalnym zakresie: a. Bieżące wykorzystanie przestrzeni w rozbiciu na: i. przestrzeń danych wykorzystywanych przez serwery (przed technologiami redukcji danych) ii. redukcja zajętości dzięki kompresji iii. redukcję zajętości dzięki deduplikacji iv. redukcję zajętości z uwagi na migawki niewymagające pełnej kopi danych v. przestrzeń danych faktycznie zajęta na macierzy vi. współczynnik redukcji danych b. Ilość otwartych dla środowiska zgłoszeń serwisowych w rozbiciu na: i. zgłoszenie dla których natychmiastowo zalecono rozwiązanie ii. zgłoszenia wymagające interakcji z serwisem c. Raport RPO zasobów chronionych migawkami w podziale na grupy aplikacyjne d. Raport Retencji (RET) zasobów chronionych migawkami w podziale na grupy aplikacyjne e. Raport odporności na katastrofy zasobów replikowanych w podziale na grupy aplikacyjne f. Rekomendacje rozbudowy wraz ze wskazaniem przyczyn dla wszystkich posiadanych macierzy Raporty muszą być udostępniane w trybie online dla uprawnionych osób oraz wysyłane na listę odbiorców email. Oferent może dostarczyć funkcjonalność jako usługę chmurową lub jako odpowiednio zwymiarowane i skonfigurowane dla oferowanego środowiska urządzenie
Monitoring i analityka	Macierz musi umożliwiać monitoring w minimalnym zakresie: a. Zdarzeń związanych z macierzą (błędów, procedur utrzymania itp.) w podziale na priorytety (co najmniej Ważny, Pilny, Krytyczny) i obszary (Pule, macierze, grupy zasobów, migawki); b. Obciążenia macierzy z rozbiciem na obciążenie procesorów i buforu macierzy; c. Zajętości urządzenia: historycznej i przewidywanych trendów z okresu 3-12 miesięcy w podziale na aplikacje (serwery wirtualne (VMware/Hyper-V), Exchange, Oracle, MS SQL, SPS, Docker), woluminy (z migawkami)

	oraz pule/grupy; d. Trendów pojemności udostępnianych zasobów (woluminy, pule/grupy) w przedziale 1-365 dni z granulacją odpowiednio 10min-24h; e. Trendów wydajności udostępnianych zasobów w przedziale 1-365 dni z granulacją odpowiednio 10min - 24h; f. Historii i bieżącego statusu zgłoszeń serwisowych; Oferent może dostarczyć funkcjonalność jako usługę chmurową lub jako odpowiednio zwymiarowane i skonfigurowane dla oferowanego środowiska urządzenie.
Ochrona inwestycji	Oferowane urządzenie musi zapewniać możliwość uaktualnienia do nowej generacji kontrolerów (bez konieczności zakupu pojemności dyskowej) w trybie „na gorąco”. Musi wspierać lub być gotowe do implementacji NVMeoF (Ethernet i/lub SAN).
Wsparcie dla technologii kontenerów	Macierz musi wspierać i oferować integrację z Docker, Red-hat Openshift, Kubernetes oraz MESOS.
Porty udostępniające usługę	Macierz musi być wyposażona minimum w dwa kontrolery z łączną ilością portów: a) 8 x 10 Gbps Macierz musi pozwalać na rozbudowę do łącznej ilości 28 portów o prędkości działania powyżej 8Gbps.
Zarządzanie jakością usług	Macierz musi zapewniać kontrolę jakości uslug (QoS) co najmniej w zakresie ograniczenia parametrów IOps i MBps z gradualnością per LUN.
Technologia Thin oraz optymalizacja wykorzystania przestrzeni.	Macierz musi zapewniać granularne (per LUN) i równoczesne funkcje efektywnego wykorzystania przestrzeni w trybie na gorąco (inline) na poziomie kontrolera: a) deduplikacji blokiem 4kB b) kompresji algorytmem LZE dla wszystkich oferowanych dysków HDD i SSD. Macierz musi umożliwiać równoczesne udostępnianie dowolnej kombinacji zdeduplikowanych, skompresowanych, niezdeduplikowanych i nieskompresowanych LUN.
Migawki macierzowe	Macierz musi wspierać tworzenie co najmniej 90 000 migawek per macierz i 800 per LUN w technologii “redirect on write”. Zamawiający dopuszcza macierze używające technologii „copy on write” pod warunkiem zastosowania współczynnika równoważności W_1=1.

	Technologia migawek musi być zgodna i integrować się z oprogramowaniem MS Exchange, MS SQL, VMware, Hyper-V, Citrix oraz Oracle w celu tworzenia koherentnych aplikacyjnie kopii zapasowych w trybie online i licencjonowania na pełną pojemność macierzy.
Zdalna replikacja	Macierz musi wspierać sprzętową replikację synchroniczną i periodyczną/asynchroniczną: a) danych z granularnością na poziomie pojedynczych LUN lub grup LUN przez sieć WAN pomiędzy ośrodkami przetwarzania b) migawek z wykorzystaniem polityk i harmonogramów Replikacji mają podlegać wyłącznie unikalne bloki danych pomiędzy dowolną kombinacją macierzy typu All Flash oraz Hybrid w co najmniej 3 ośrodkach przetwarzania.
Licencje	Macierz powinna być dostarczona z licencją na wszystkie krytyczne funkcjonalności do pełnej pojemności macierzy w tym co najmniej: tworzenia migawek sprzętowych zarządzanych przez aplikację, klonów, replikacji, QoS, tiering danych, zarządzanie i monitoring.
Fizyczne wymiary rozwiązania	Oferowana macierz musi zajmować maksymalnie wysokość 4U w szafie RACK.
Usługi gwarancyjne	W razie awarii i wymiany dysków HDD/SSD/Flash w macierzy, uszkodzone dyski pozostają u Zamawiającego. W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy. Nośniki SSD objęte są usługami wsparcia nieograniczonymi intensywnością wykorzystania (bez względu na intensywność zapisów).

II.1.5 Biblioteka LTO

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

CECHA	WYMAGANIA MINIMALNE
Obudowa	Maksymalnie 3U RACK 19 cali (wraz z szynami montażowymi)
Napęd taśmowy	Urządzenie musi być wyposażone w jeden napęd LTO-7 z interfejsem SAS. Musi przy tym zapewniać wydajność co najmniej 300 MB/s oraz

	pojemność pojedynczej taśmy co najmniej 6 TB (parametry podane bez kompresji danych). Urządzenie musi umożliwiać zainstalowanie drugiego napędu LTO-7.
Sloty na taśmy	Urządzenie musi być wyposażone w co najmniej 24 sloty na taśmy magnetyczne LTO. Oferowane urządzenie musi posiadać możliwość konfiguracji co najmniej jednego tzw. „mail slot" umożliwiającego wymianę pojedynczej taśmy bez konieczności wyjmowania z biblioteki całego magazynka z taśmami.
Czytnik kodów kreskowych	Urządzenie musi być wyposażone w czytnik kodów kreskowych.
Zarządzanie	Urządzenie musi posiadać możliwość zdalnego zarządzania za pośrednictwem przeglądarki internetowej.
Szyfrowanie danych	Urządzenie powinno mieć możliwość rozbudowy o mechanizm sprzętowego szyfrowania danych z możliwością zabezpieczenia kluczy szyfrujących na nośniku USB.
Połączenia kablowe	Wraz z urządzeniem należy dostarczyć odpowiedni kabel umożliwiający dołączenie go do oferowanego serwera backupu.
Niezawodność działania	Dla oferowanego autoloadera taśmowego parametr MTBF musi wynosić co najmniej 100 000 godzin. Dla oferowanego autoloadera taśmowego parametr MSBF musi wynosić co najmniej 2 000 000 pełnych cykli „załaduj/wyładuj"
Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.
Taśmy	Razem z urządzeniem należy dostarczyć minimum 15 szt. taśm LTO-7 do wielokrotnego zapisu wraz z dedykowanymi etykietami z kodami kreskowymi, obsługiwanymi przez wbudowany w bibliotekę czytnik. Razem z urządzeniem należy dostarczyć minimum 1 szt taśmy czyszczącej do napędu LTO-7.

II.1.6 Przełącznik zasobowy do macierzy

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

CECHA	WYMAGANIA MINIMALNE
Opis techniczny	1. Typ i liczba portów: Minimum 48 portów 1G/10GbE SFP+ umieszczonych z przodu obudowy Minimum 6 portów 40GbE QSFP+ Wszystkie porty muszą być od siebie niezależne, nie dopuszcza się portów typu Combo 2. Wbudowany, dodatkowy, dedykowany port Ethernet do zarządzania poza pasmem - out of band management 3. Port konsoli RS232 ze złączem DB9 lub RJ45 4. Port USB 2.0 5. Przepustowość minimum 1000 Mpps dla pakietów 64 bajtowych 6. Wydajność: minimum 1400 Gbps (prędkość przełączania „wirespeed" dla każdego portu przełącznika) 7. Przełączanie w warstwie 2 i 3 modelu OSI 8. Wielkość bufora pakietów (packet buffer): minimum 12 MB 9. Minimum 512MB pamięci typu Flash 10. Minimum 2GB pamięci operacyjnej 11. Przełącznik wyposażony w redundantne, modularne wentylatory (minimum dwa niezależne moduły wentylatorów) 12. Przepływ powietrza w przełączniku musi odbywać się w kierunku z przodu przełącznika do tyłu przełącznika. Nie dopuszczalne są rozwiązania, z mieszanym przepływem powietrza. 13. Dwa wbudowane (wewnętrzne, modularne) zasilacze AC dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia. 14. 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 320 portów 10GbE SFP+. Topologia

CECHA	WYMAGANIA MINIMALNE
	stosu musi zapewniać redundancję (połączenia typu pierścień lub mesh, nie dopuszcza się topologii typu łańcuch (daisy-chain)). 15. Łączenie w stos z wykorzystaniem portów 10Gb, 40Gb i agregowanych portów 10Gb (w celu zwiększenia przepustowości w stosie) 16. Realizacja łączy agregowanych w ramach różnych przełączników będących w stosie 17. Tablica adresów MAC o wielkości minimum 128 000 pozycji 18. Obsługa ramek Jumbo 19. Obsługa Quality of Service 20. Obsługa mechanizmów: strict priority (SP) queuing, weighted fair queuing (WFQ), weighted random early discard (WRED), SP+WFQ 21. Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol 22. Obsługa sieci IEEE 802.1Q VLAN – 4094 sieci VLAN oraz IEEE 802.1ad QinQ 23. Obsługa IGMP v1/v2/v3, IGMP Snooping v1/v2/v3, PIM DM, PIM SM, MLD snooping v1/v2 oraz IPv6 PIM Snooping 24. Wsparcie dla FibreChannel over Ethernet (FCF/Transit/NPV) 25. Wsparcie dla Data Center Bridging (DCB): • IEEE 802.1Qbb Priority Flow Control (PFC) • Data Center Bridging Exchange (DCBX) 26. Routing IPv4 – statyczny i dynamiczny (min. RIP, IS-IS, OSPF, BGP) 27. Routing IPv6 – statyczny i dynamiczny (min. RIPng, IS-ISv6, OSPFv3) 28. Obsługa ECMP (Equal Cost Multi Path) 29. Tablica routingu o pojemności co najmniej 1000 wpisów 30. Serwer DHCP, klient DHCP, obsługa opcji 82 (snooping i relay), DHCP snooping 31. Obsługa list ACL na bazie informacji z warstw 3/4 modelu OSI. Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia 32. Obsługa standardu 802.1p

CECHA	WYMAGANIA MINIMALNE
	33. Możliwość zmiany wartości pola DSCP i/lub wartości priorytetu 802.1p 34. Funkcje mirroringu: 1 to 1 Port mirroring, Many to 1 port mirroring, remote mirroring 35. Obsługa funkcji logowania do sieci („Network Login") zgodna ze standardem IEEE 802.1x 36. Możliwość centralnego uwierzytelniania administratorów na serwerze RADIUS 37. Zarządzanie poprzez port konsoli, SNMP v.1, 2c i 3, Telnet, SSH v.2 38. Syslog 39. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) oraz LLDP-MED 40. Obsługa sFlow 41. Obsługa protokołu OpenFlow w wersji, co najmniej, 1.3 42. Obsługa Network Time Protocol (NTP), Simple Network Time Protocol (SNTP) oraz kompatybilność z Precision Time Protocol (PTP) RFC 1855 43. Obsługa OAM (IEEE 802.3ah) 44. Obsługa CFD (IEEE 802.1ag) 45. Modularny system operacyjny ze wsparciem dla In Services Software Upgrade (ISSU) i skryptów w języku Python 46. Przechowywanie wielu wersji oprogramowania na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch wersji oprogramowania). 47. Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji). 48. Funkcja wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym

CECHA	WYMAGANIA MINIMALNE
	urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nowa konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiast - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian. 49. Wysokość w szafie 19" – 1U o głębokości maksymalnie 70 cm 50. Maksymalny pobór mocy nie większy niż 350W 51. Minimalny zakres temperatur pracy od 0°C do 40°C
Wyposażenie	• Każdy przełącznik musi być wyposażony w 2 wkładki 40G QSFP+ pracujące na światłowodach jedno-modowych (SM) na odległość minimum 2 km • Każdy przełącznik musi być wyposażony w wkładkę optyczną 10G SR ze złączem LC, pracującą na światłowodach wielomodowych • Każdy przełącznik musi być wyposażony w 4 wkładki optyczne 1G SX ze złączem LC, pracujące na światłowodach wielomodowych • Każdy przełącznik powinien być wyposażony w 4 wkładki 1G Base-T (RJ45) • Każdy przełącznik powinien być wyposażony w 2 kable DAC 10G SFP+ o długości 3m

II.1.7 Zasilacz awaryjny UPS

Wymagane dostarczenie 1 szt. UPS i podłączenie do rozdzielni elektrycznej w pomieszczeniu serwerowni głównej i rozdzielni spełniających poniżej opisane minimalne parametry funkcjonalne:

Cecha	Wymagania minimalne
Moc pozorna	5000 VA
Moc rzeczywista	4500 W
Topologia (klasyfikacja IEC 62040-3)	On-line z korekcją współczynnika mocy
Sprawność przy pracy	>94 %

normalnej (100% obc.)	
Sprawność w trybie podwyższonej sprawności (100% obc.)	>98 %
Współczynnik mocy	0,9
Czas przełączenia na baterię	0 ms
Liczba, typ gniazd wyjściowych	Listwa zaciskowa, 8 x IEC C13 (2 grupy gniazd sterowalnych za pomocą oprogramowania oraz z poziomu wyświetlacza po 4 x IEC C13), 2 x IEC C19 16A
Typ gniazda wejściowego	Listwa zaciskowa
Czas podtrzymania dla 100% obciążenia dla pf=0,9	20 min
Czas podtrzymania przy 50% obciążenia dla pf=0,9	48 min
Dodatkowe baterie	Możliwość dodania do 4 dodatkowych modułów baterii w celu wydłużenia czasu podtrzymania do 80 minut dla 100% obciążenia przy pf=0,9
Napięcie znamionowe	200/208/220/230/240 V
Tolerancja napięci prostownika	176V – 276 V (100-276V przy obniżonej mocy)
Częstotliwość znamionowa	50/60 Hz autodetekcja
Tolerancja częstotliwości	40– 70 Hz
Kształt napięcia	Sinusoidalny
Napięcie znamionowe wyjściowe	230 V (domyślnie) / możliwość wyboru 200/208/220/240 V
Zakres zmian napięcia	+/-1% napięcia nominalnego
Częstotliwość wyjściowa	50/60 Hz +/-0,5%
Współczynnik szczytu	3:1
Dopuszczalny zakres współczynnika mocy obc. Liniowego	0,5 indukcyjny - 0,5 pojemnościowy
Baterie wymieniane przez użytkownika "na gorąco"	Tak
Ochrona przed przeładowaniem	Tak (ograniczenie prądu ładowarki, wyłączenie ładowarki / alarm)
Ochrona przed głębokim	Tak

rozładowaniem	
Okresowy automatyczny test baterii	Tak
Zdolność zwarciowa	90A
Możliwość uruchomienia bez napięcia w sieci	Tak
Baterie wewnętrzne UPSa o pojemności nie mniejszej niż	5Ah 12V, minimum 15 szt.
Interfejs komunikacyjny	• USB
	• RS232 DB-9 żeński (HID)
	• styki przekaźnikowe
	• miniport wyłącznik ON/OFF
	• SNMP/Ethernet
Panel sterowania z wyświetlaczem LCD	• Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPSa). Dostarcza informacji o: stanie pracy urządzenia, stanie obciążenia, pomiarach i ustawieniach. Funkcje ustawień i odczytów: lokalne, wyjścia (napięcie wyjściowe, częstotliwość wyjściowa), baterii (test baterii), pomiary i dane (numer seryjny, napięcie i częstotliwość wejściowa i wyjściowa, poziom obciążenia, pozostały czas podtrzymania, wydajność, zużycie energii).
	• Poziomy rząd przycisków sterowania
	• Poziomy rząd wskaźników stanu : zasilanie z siec(zielony), trybu bateryjnego (żółty), usterki (czerwony)
	• Sygnalizator akustyczny
Sygnały akustyczne	• Awaria
	• Niski stan naładowania baterii
	• Przeciążenie
	• Serwis
Przyciski sterujące i wskaźniki diodowe LED	• Przycisk Escape (anulowanie)
	• Przyciski funkcyjne (przewijanie w górę i w dół)
	• Przycisk Enter (potwierdzający)
	• Przycisk ON/OFF załączenia i wyłączenia
	• LED trybu zasilania z sieci (kolor zielony)
	• LED trybu baterii (kolor żółty)
	• LED usterki (kolor czerwony)

Kolor	Czarny RAL 9005
Typ obudowy	Uniwersalna Tower/Rack 3U
Wyposażenie standardowe	UPS, instrukcja obsługi(CD), instrukcja bezpieczeństwa
	1 x kabel szeregowy RS-232,
	1 x kabel komunikacyjny USB
	2 x kable wyjściowe IEC 10A
	2 x uchwyty kablowe
	1 x zestaw szyn montażowych 19’
	1 x podstawki do montażu wieżowego
	1x karta sieciowa SNMP/Ethernet
Zgodność ze standardem Energy Star	Tak
Maksymalna szerokość	440 mm
Maksymalna wysokość	260 mm
Maksymalna głębokość	685 mm
Maksymalny ciężar	116 kg
Poziom hałasu w odl. 1m	do 45 dBA dla pracy normalnej
Znaki bezpieczeństwa	CE, C-Tick, UL
Parametry karty sieciowej	
Network Support	Ethernet /10Mbps - Half duplex - 10Mbps - Full duplex - 100Mbps - Half duplex - 100Mbps - Full duplex - 1.0 Gbps - Full duplex / HTTP 1.1, SNMP V1, SNMP V3/ NTP, SMTP, DHCP/
Protokoły	MQTT/RNDIS/LDAP/NVD/SSH/PKI
Szyfrowanie	pakiet szyfrów TLS 1.2 z minimum SHA256
Tymczasowe hasła	Nadawanie użytkownikowi dostępu za pomocą konta. Konto może wygasać po odpowiedniej, wprowadzonej liczbie dni (hasło przestaje być aktywne)
Certyfikaty	CA, UL 290-2-2
Funkcje:	komunikacja Web/SNMP
Kompatybilny z:	SNMP v1/v3 i IP v4/v6
Port USB	MicroUSB (port serwisowy)
Interfejs	HTML5
Network Support	Ethernet /10Mbps - Half duplex - 10Mbps - Full duplex - 100Mbps - Half duplex - 100Mbps - Full duplex - 1.0 Gbps - Full duplex / HTTP 1.1, SNMP

	V1, SNMP V3/ NTP, SMTP, DHCP/
Adresowanie IP	DHCP/BootP/Manualne
Obsługiwane MIB	MIB II - Standard IETF UPS MIB (RFC 1628) –Eaton PowerMib (XUPS.MIB)
Systemy operacyjne obsługiwane przy zamykaniu systemu	Microsoft Windows, UNIX i Linux
Certyfikaty	CA, UL 2900-2-2
Konfiguracja e-mail	SMTP
Protokoły	MQTT/RNDIS/LDAP/NVD/SSH/PKI
Szyfrowanie	pakiet szyfrów TLS 1.2 z minimum SHA256
Panel HMI	Tak
Kompatybilność z ICS	IDPS/ SCADA
Tymczasowe hasla	Nadawanie użytkownikowi dostępu za pomocą konta. Konto może wygasać po odpowiedniej, wprowadzonej liczbie dni (hasło przestaje być aktywne)
Blokowanie konta	Po określonej liczbie nieudanych prób wpisania hasła lub określonej liczbie dni.

II.1.8 Szafa Rack

Wymagane jest dostarczenie 1 szt. szafy rack spełniającej poniższe wymagania minimalne:

CECHA	WYMAGANIA MINIMALNE
Wysokość	Nie mniejsza niż 42U
Nośność	Nie mniejsza niż ~~1000~~ **450** kg.
Szerokość całkowita	800 mm.
Głębokość całkowita	1200 mm.
Drzwi przednie oraz tylnie	Stal perforowana.
Wyposażenie szafy	- 2x półka; - 2x organizer - 1x listwa zasilająca RACK 19” 1U z wtykiem IEC C14 z wyłącznikiem zabezpieczonym przed przypadkowym wyłączeniem, minimum 8 gniazd typu E, zestaw śrub mocujących wraz z koszyczkami i podkładkami; - 1 x listwa zasilająca RACK 19” 1U z wtykiem CEE 7/7 z wyłącznikiem

CECHA	WYMAGANIA MINIMALNE
	zabezpieczonym przed przypadkowym wyłączeniem, minimum 8 gniazd typu E, zestaw śrub mocujących wraz z koszyczkami i podkładkami; - mikroprocesorowy panel sterowania wentylatorami oraz panel wentylacyjny dachowy z min. 4 wentylatorami; - 4x nóżki + 4x kółka

II.1.9 Przełącznik LAN

Wymagane jest dostarczenie 1 szt. przełącznika spełniających poniżej opisane minimalne parametry funkcjonalne.

CECHA	WYMAGANIA MINIMALNE
Opis techniczny	1. Minimum 24 porty 10BASE-T/100BASE-TX/1000BASE-T 2. Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP). 3. Przepustowość: minimum 128 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika) 4. Wydajność: minimum 95 Mp/s 5. Tablica adresów MAC o wielkości minimum 16000 pozycji 6. Bufor pakietów nie mniejszy niż 12 MB 7. Pamięć stała (typu Flash): minimum 2 GB 8. Pamięć operacyjna: minimum 1 GB 9. Obsługa ramek Jumbo 10. Routing IPv4 – minimum: statyczny (minimum 1000 tras), RIP 11. Routing IPv6 – minimum: statyczny (minimum 500 tras), RIPng 12. Policy Based Routing 13. Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping 14. Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol 15. Obsługa sieci IEEE 802.1Q VLAN – minimum 512 jednoczesnych sieci VLAN 16. Funkcja Root Guard umożliwiająca ochronę sieci przed wprowadze-

	niem do sieci urządzenia, które może przejąć rolę przełącznika Root dla protokołu Spanning Tree 17. BPDU Guard lub odpowiednik– funkcja umożliwiająca wyłączenie portów Fast Start w momencie odebrania na tym porcie ramek BD-PU w celu przeciwdziałania pętlom 18. Wsparcie dla funcji DHCP server, DHCP Relay, DHCP client oraz DHCP Snooping (wszystkie dla IPv4 i IPv6) 19. Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI 20. Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia 21. Obsługa standardu 802.1p – min. 8 kolejek na porcie 22. Możliwość zmiany wartości pola DSCP i wartości priorytetu 802.1p 23. Możliwość wyboru sposobu obsługi kolejek – Strict Priority (SP); Weighted Round Robin (WRR) lub podobny algorytm; 24. Możliwość ograniczania pasma na porcie 25. Funkcja mirroringu portów 26. Obsługa funkcji logowania do sieci („Network Login") zgodna ze standardem IEEE 802.1x: • Możliwość przydziału stacji do wskazanej sieci wirtualnej podczas logowania IEEE 802.1x • Możliwość uwierzytelniania wielu użytkowników na jednym porcie • Przypisanie profilu QoS dla użytkownika lub grupy użytkowników 27. LLDP - IEEE 802.1AB Link Layer Discovery Protocol oraz LLDP-MED 28. TACACS+ i RADIUS Network Login 29. RADIUS Accounting 30. Możliwość centralnego uwierzytelniania administratorów na serwerze RADIUS 31. Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https 32. Syslog 33. Obsługa sFlow lub NetFlow 34. Obsługa NTP 35. Przechowywanie wielu wersji oprogramowania na przełączniku

	36. Przechowywanie wielu plików konfiguracyjnych na przełączniku 37. Funkcja wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nowa konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiast - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian. 38. Wsparcie dla mechanizmu typu DLDP - Data Link Detection Protocol 39. Ochrona przed sztormami pakietowymi (broadcast, multicast, unicast), z możliwością definiowania wartości progowych 40. Minimalny zakres pracy od 0°C do 45°C 41. Wysokość w szafie 19" – 1U, głębokość nie większa niż 45 cm 42. Maksymalny pobór mocy nie większy niż 100W
Wyposażenie	• Przełącznik powinien być wyposażony w 2 kable DAC 10G SFP+ o długości 3m

II.1.10 Przełącznik Zarządzający

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

CECHA	WYMAGANIA MINIMALNE
Opis techniczny	- Minimum 24 porty 10/100/1000BaseT - Minimum 4 porty Gigabitowe SFP, niezależne od wymaganych portów 10/100/1000BaseT - Automatyczne wykrywanie przeplotu (AutoMDIX) na portach 100/1000BaseT - Wydajność przełączania co najmniej 56 Gbps oraz przepustowość 41,6 Mpps dla pakietów 64 bajtowych - Obsługa 4094 tagów IEEE 802.1Q oraz minimum 512 jednoczesnych sieci VLAN - Funkcja łączenia w stosy (klaster) pozwalająca co najmniej na zarządzanie z

	poziomu jednego adresu IP minimum 9 urządzeniami. Jeżeli funkcja ta wymaga dodatkowych licencji, modułów lub kabli to Zamawiający wymaga ich dostarczenia w ramach tego postępowania. - Funkcja automatycznej aprowizacji i konfiguracji przełącznika przy jego pierwszym podłączeniu do sieci bez konieczności wykonywania wstępnej, ręcznej konfiguracji - Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az - Bufor pakietów nie mniejszy niż 1,5MB - Minimum 128MB pamięci Flash - Dostęp do urządzenia przez konsolę szeregową (linia komend umożliwiająca pełne zarządzanie przełącznikiem), HTTPS, SSHv2 i SNMPv3 - Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s) - Obsługa Secure FTP - Obsługa 802.3ad Link Aggregation Protocol (LACP) - Obsługa Simple Network Time Protocol (SNTP) v4 lub NTP - Wielkość tablicy adresów MAC: minimum 16000 - Obsługa LLDP i LLDP-MED - Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 4 kolejek sprzętowych, rate-limiting - Funkcja autoryzacji użytkowników zgodna z 802.1x - Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+, - Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection) - Obsługa list kontroli dostępu (ACL) - Obudowa wieżowa 1U umożliwiająca instalację w szafie 19" o głębokości nie większej niż 45 cm. - Maksymalny pobór mocy nie większy niż 60W - Minimalny zakres pracy od 0°C do 45°C
Inne	Dopuszczalne jest zastosowanie wkładek światłowodowych SFP+ innego producenta niż przełączniki.

II.1.11 Punkty dostępowe wewnętrzne

Wymagane jest dostarczenie 6 szt. punktów dostępowych spełniających opisane minimalne parametry techniczne

CECHA	WYMAGANIA MINIMALNE
Parametry podstawowe	1. Punkt dostępowy musi być przeznaczony do montażu wewnątrz budynków. Musi być wyposażony w dwa niezależne moduły radiowe, pracujące w paśmie 5GHz a/n/ac/ac wave 2 oraz 2.4GHz b/g/n; 2. Punkt dostępowy musi mieć możliwość współpracy z centralnym kontrolerem sieci bezprzewodowej w infrastrukturze; 3. Punkt dostępowy musi posiadać funkcjonalność zarządzania przez przeglądarkę internetową z wykorzystaniem protokołu http/https/telnet/ssh 4. Punkt dostępowy musi mieć możliwość pracy w trybie monitorującym pasmo radiowe w celu wykrywania np. fałszywych AP; 5. Punkt dostępowy musi mieć możliwość pracy jako analizator widma; 6. Wsparcie dla RADIUS; 7. Musi istnieć możliwość integracji z zewnętrznymi serwerami uwierzytelniania RADIUS lub TACACS.; 8. Punkt dostępowy musi obsługiwać nie mniej niż 8 niezależnych SSID per radio; 9. Każde SSID musi mieć możliwość przypisania do sieci VLAN; 10. **Punkt dostępowy musi mieć możliwość obsługi trybu pracy bez kontrolera**
Zarządzanie pasmem radiowym	1. Zarządzanie pasmem radiowym w sieci punktów dostępowych musi się odbywać automatycznie za pomocą auto-adaptacyjnych mechanizmów. 2. Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe 3. Stałe monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu 4. Rozkład ruchu pomiędzy różnymi punkami dostępowym oraz pasmami bazując na ilości użytkowników oraz utylizacji pasma 5. Wykrywanie interferencji oraz miejsc bez pokrycia sygnału 6. Automatyczne przekierowywanie klientów, którzy mogą pracować w pasmie 5GHz 7. Wyrównywanie czasów dostępu do pasma dla klientów pracujących w

	standardzie 802.11n/ac wave 2 oraz starszych (802.11b/g) 8. Wsparcie dla 802.11d oraz 802.11h
Pozostałe parametry sieciowe	1. Minimalizacja interferencji związanych z sieciami 3G/4G LTE; 2. Obsługa roamingu klientów w warstwie 2; 3. Obsługa monitoringu przez SNMP; 4. Obsługa logowania na zewnętrznym serwerze SYSLOG; 5. Punkt dostępowy musi posiadać wbudowane anteny do pracy w trybach 2×2:2 @ 2.4 GHz, 2x2:2 @ 5 GHz, BLE antenna 6. Obsługa standardów 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac wave 2 7. Specyfikacja radia 802.11a/n/ac wave 2 a) Obsługiwane częstotliwości – 5.150 ~ 5.250 GHz (low band) – 5.250 ~ 5.350 GHz (mid band) – 5.470 ~ 5.725 GHz (Europa) – 5.725 ~ 5.850 GHz (high band) b) Typy modulacji: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM c) Moc transmisji konfigurowalna przez administratora – możliwość zmiany co 1dbm d) Prędkości transmisji: – 6, 9, 12, 18, 24, 36, 48, 54 Mbps dla 802.11a – MCS0-MCS15 (6,5Mbps do 300Mbps) dla 802.11n (2,4 GHz) – MCS0-MCS9, NSS = 1-**2** ~~3~~ (6.5 Mbps do ~~1300~~ **867 Mbps**) dla 802.11ac e) Obsługa HT – kanały 20/40MHz dla 802.11n f) Obsługa VHT – kanały 20/40/80MHz dla 802.11ac g) Wsparcie dla technologii DFS (Dynamic frequency selection) h) Agregacja pakietów: A-MPDU, A-MSDU dla standardów 802.11n/ac 8. Specyfikacja radia 802.11b/g/n: a) Częstotliwość 2,400 ~2,4835 b) Typy modulacji – CCK, BPSK, QPSK,16-QAM, 64-QAM

	c) Moc transmisji konfigurowalna przez administratora d) Prędkości transmisji: – 1,2,5.5,11 Mbps dla 802.11b – 6,9,12,18,24,36,48,54 Mbps dla 802.11g 9. Punkt dostępowy musi posiadać co najmniej a) 1 interfejs 10/100/1000 Base-T b) zasilanie PoE 48V DC zgodne z 802.3af/802.3at lub z zasilacza c) przycisk przywracający konfigurację fabryczną d) Kontrolka LED do określania statusu systemu i interfejsów radiowych 10. Parametry pracy urządzenia: a) Temperatura otoczenia: 0-~~45~~ **40** º C b) Wilgotność 5% - 93% nie skondensowana c) Znak CE, EN 60601-1-x 11. Urządzenie musi posiadać certyfikat Wi-Fi Alliance (WFA) dla standardów 802.11/a/b/g/n/ac 12. Punkt dostępowy musi zostać dostarczony z elementami montażowymi niezbędnymi do montażu na płaskiej powierzchni.
Dodatkowe wyposażenie	Do każdego punktu dostępowego należy dostarczyć zasilacz PoE.

II.1.12 UTM

1. Wymagane jest dostarczenie 1 szt. zapory ogniowej spełniającej poniżej opisane minimalne parametry funkcjonalne.
2. W ramach realizacji zamówienia Wykonawca dostarczy, skonfiguruje, wdroży i uruchomi zaporę ogniową zgodnie z założeniami:

- Zapora zostanie fizycznie zainstalowana w wyznaczonym miejscu.
- Należy wykonać upgrade firmware zapory do najnowszej stabilnej wersji oprogramowania.
- Zapora zostanie dołączona do klastra/stosu przełączników macierzowych (rdzeń).
- Firewall zostanie zaadresowana zgodnie z przydzielonymi przez administratorów ośrodka adresami IP.
- Należy skonfigurować routing na zaporze zgodnie z zaleceniami administratorów ośrodka.
- Należy skonfigurować dostęp do urządzeń SSH oraz HTTPS, wygenerować w tym celu odpowiednie klucze RSA/DSA oraz certyfikaty.
- Należy skonfigurować niezbędne agregacje na portach przełączników macierzowych/rdzeniowych.

- Należy skonfigurować wszystkie wymagane sieci wirtualne VLAN w obrębie całej sieci oraz interfejsy VLAN.
- Sieci vlan należy przypisać do portów zgodnie z wymaganiami.
- Należy skonfigurować zabezpieczenia dostępu do zapory sieciowej.
- Należy skonfigurować użytkowników – administratorów lokalnych na urządzeniach.
- Należy skonfigurować polityki bezpieczeństwa zgodnie z tzw. Best-practices oraz zaleceniami ośrodka.
- Należy skonfigurować sieć DMZ.
- Należy skonfigurować funkcję NAT.
- Należy skonfigurować usługi VPN, IPS, antywirus, web filtering itp. zgodnie z zaleceniami i tzw. best-practices.

CECHY	WYMAGANIA MINIMALNE
Wymagania Ogólne	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 10 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. Protokołów routingu dynamicznego.
Redundancja, monitoring i	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Ac-

wykrywanie awarii	tive-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie:	1. System realizujący funkcję Firewall musi dysponować minimum: • 20 portami Gigabit Ethernet RJ-45. • 2 gniazdami SFP 1 Gbps. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie AC. 5. Musi posiadać dysk **min 480 GB SSD** na którym będą zbierane oraz zapisywane logi i możliwość zapisywania logów na wskazanym serwerze logów.
Parametry wydajnościowe:	1. W zakresie Firewall'a obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 30.000 nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 7.4 Gbps. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1 Gbps. 4. Wydajność szyfrowania IPSec VPN: nie mniej niż 4 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 500 Mbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 250 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 130 Mbps
Funkcje Systemu	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie

Bezpieczeństwa:	poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL. 12. Analiza ruchu szyfrowanego protokołem SSH.
Polityki, Firewall	1. System Firewall musi umożliwiać tworzenie list kontroli dostępu realizowanych bezstanowo przed funkcją FW. 1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu.

	• Dedykowany ALG (Application Level Gateway) dla protokołu SIP. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
Połączenia VPN	1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2. • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19 i 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling” dla połączeń Client-to-Site. 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
Routing i obsługa łączy WAN	1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego. • Policy Based Routingu. • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. 2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

Zarządzanie pasmem	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Kontrola Antywirusowa	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
Ochrona przed atakami	1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 6500 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty)

	oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2500 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur
Kontrola WWW	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.

	• Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
Logowanie	1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

	3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. Musi istnieć możliwość logowania do serwera SYSLOG.
Serwisy i usługi	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i usług. Powinny one obejmować: a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy.

II.2 Oprogramowanie systemowe i narzędziowe

II.2.1 Oprogramowanie systemowe - komplet

Specyfikacja techniczna oprogramowania do wirtualizacji serwerów, serwerów bazodanowych i serwera kopii zapasowych.

Oprogramowanie systemowe musi posiadać następujące, wbudowane cechy:

WYMAGANIA MINIMALNE	
Wymagania funkcjonalno-techniczne (minimalne):	1. Należy dostarczyć licencje na oprogramowanie do wirtualizacji dla dwóch serwerów wirtualizacji w ilości odpowiedniej dla dostarczanych procesorów i/lub rdzeni. 2. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych. 3. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej. 4. Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne wyposażone w 512 logicznych wątków oraz do 24 TB pamięci fizycznej RAM. 5. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1 – 240

	procesorowych. 6. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB. 7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 12 TB pamięci operacyjnej RAM. 8. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z których każda może mieć 1 – 8 wirtualnych kart sieciowych. 9. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. 10. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. 11. Rozwiązanie musi umożliwiać poprawne zainstalowanie następujących systemów operacyjnych: Windows Server 2008 R2, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows 7, Windows 10, SLES 12, SLES 15, RHEL 6, RHEL 7, Debian 8, Debian 9, CentOS 6, CentOS 7, FreeBSD, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04 12. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. 13. Rozwiązanie powinno posiadać konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. 14. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) 15. Oprogramowanie do wirtualizacji powinno zapewnić

	możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy. 16. Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory. 17. Rozwiązanie musi zapewniać mechanizm replikacji oraz klonowania wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych. 18. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA), aby w przypadku awarii lub niedostępności serwera hosta wirtualizacji, wybrane przez administratora i uruchomione nim wirtualne maszyny zostały automatycznie uruchomione na innych serwerach hostach. 19. System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. 20. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej oraz agregację przepustowości tych kart. Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN).
Specyfikacja oprogramowania – systemów operacyjnych dla maszyn wirtualnych.	Należy dostarczyć licencje na systemy operacyjne dla serwerów hostów wirtualizacji, umożliwiające uruchomienie na każdym z nich minimum 2 maszyn wirtualnych z systemem Windows Server 2019, sumarycznie minimum 4 maszyn wirtualnych w całym klastrze. Należy dostarczyć odpowiednią ilość licencji na rdzenie, dostosowaną do zainstalowanych procesorów w serwerach hostach wirtualizacji. Licencje muszą pozwalać na przypisanie ich do dowolnego serwera Zamawiającego. Wraz z licencjami na systemy

	operacyjne, należy dostarczyć sumarycznie **min. 80 licencji dostępowych na użytkownika** do tych systemów operacyjnych.
Specyfikacja oprogramowania – system operacyjny serwera kopii zapasowych.	Należy dostarczyć licencje na system operacyjny dla serwera kopii zapasowych. Jeżeli jest to wymagane, to należy dostarczyć odpowiednią ilość licencji na rdzenie, dostosowaną do zainstalowanych procesorów w serwerze kopii zapasowych. System operacyjny serwera kopii zapasowych musi być zgodny z oferowanym rozwiązaniem do wykonywania kopii zapasowych i umożliwiać jego, w pełni funkcjonalne, uruchomienie.

II.2.2 Oprogramowanie do robienia kopii zapasowych

Należy dostarczyć licencje w ilości wymaganej do zabezpieczenia całego dostarczanego środowiska klastra wirtualizacji (na 2 serwery hosty) oraz bazodanowego (na 2 serwery hosty) – 1 kpl.

Minimalne wymagania na oprogramowanie do robienia kopii zapasowych:

WYMAGANIA MINIMALNE	
Wymagania ogólne	• Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7 oraz 7 oraz Microsoft Hyper-V 2012, 2012 R2, 2016 i 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej • Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami. • Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami. • Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V
Całkowite koszty posiadania	• Oprogramowanie musi być licencjonowanie w modelu “per-CPU” lub „per-serwer”. Wszystkie funkcjonalności zawarte w tym dokumencie powinny być zapewnione w tej licencji. Jakiekolwiek dodatkowe licencjonowanie (per zabezpieczony TB, dodatkowo płatna deduplikacja) nie jest

	dozwolone • Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej • Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków • Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji • Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla co najmniej trzech pamięci masowych w takiej puli. • Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. • Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania • Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia • Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP. W środowisku VMware musi mieć możliwość aktualizacji pola „notatki” na wirtualnej maszynie • Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota. • Oprogramowanie musi zapewniać bezpośrednią integrację z VMware vCloud Director 5.5, 5.6, 8.0, 8.10, 8.20, 9.0 oraz 9.1 i archiwizować metadane vCD. Musi też umożliwiać odtwarzanie tych metadanych do vCD. • Oprogramowanie musi mieć wbudowane mechanizmy backupu

	konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji • Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji • Oprogramowanie musi oferować zarządzanie kluczami w przypadku utraty podstawowego klucza • Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX) • Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
Wymagania RPO	• Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej • Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych • Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora • Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn • Oprogramowanie musi mieć możliwość wydzielenia osobnej roli typu tape server • Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej • Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) • Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC. • Oprogramowanie musi umieć korzystać z protokołu Catalyst w przypadku

	gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC. • Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 z systemem pliku ReFS jako repozytorium backupu. • Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. • Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik • Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding) • Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V • Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN) • Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere • Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing)
Wymagania RTO	• Oprogramowanie musi umożliwić uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. Dla środowiska vSphere powinien być wykorzystany wbudowany w oprogramowanie serwer NFS. Dla Hyper-V powinna być zapewniona taka sama funkcjonalność realizowana wewnętrznymi mechanizmami oprogramowania • Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką

	migrację swoimi mechanizmami • Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków • Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure. • Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików • Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. • Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików: ○ **Linux** ▪ ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs ○ **BSD** ▪ UFS, UFS2 ○ **Solaris** ▪ ZFS, UFS ○ **Mac** ▪ HFS, HFS+ ○ **Windows** ▪ NTFS, FAT, FAT32, ReFS ○ **Novell OES** ▪ NSS • Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces. • Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. • Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD. • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft

	Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"), • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. Opcja odtworzenia elementów, witryn, uprawnień. • Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux. • Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia. • Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych. • Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows • Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
Ograniczenie ryzyka	• Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. • Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem • Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere
Monitoring	• System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich • System musi umożliwiać monitorowanie środowiska wirtualizacyjnego

	VMware w wersji 4.1, 5.x, 6.0, 6.5, 6.7 oraz 7 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie • System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2 oraz 2016 i 2019 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. • System musi mieć status „VMware Ready" i być przetestowany i certyfikowany przez VMware • System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter • System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn • System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel • System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk • System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora • System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów • System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard) • System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna • System musi zapewnić możliwość podłączenia się do wirtualnej maszyny

	(tryb konsoli) bezpośrednio z narzędzia monitorującego • System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta • System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. • System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware • System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 5.5, 5.6, 8.0, 8.1 oraz 9.1
Raportowanie	• System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 4.1, 5.x, 6.0, 6.5, 6.7 oraz 7, vCenter Server 4.1, 5.x, 6.0, 6.5 oraz 6.7 jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2 i 2016, 2019. • System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów. • System musi być certyfikowany przez VMware i posiadać status „VMware Ready” • System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V • System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF • System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc • System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez

	administratora interwałach • System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów • System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych • System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych • System musi mieć możliwość analizowania „przeszacowanych" wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury • System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta • System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych. • System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if'. • System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware • System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots) • System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

II.3 Dostawa i wdrożenie oprogramowania dla Szpitalnego Systemu Informatycznego SSI

II.3.1 Wymogi dotyczące interoperacyjności lub migracji dla oferowanego SSI

1. Wykonawca zobowiązuje się dostarczyć Zamawiającemu wymagane funkcjonalności SSI, poprzez rozbudowanie istniejącego systemu o nowe funkcjonalności w taki sposób, aby w jak najszerszym zakresie zostały zaspokojone potrzeby Zamawiającego. Zamawiający dopuszcza wymianę posiadanego rozwiązania wyłącznie pod warunkiem zachowania pełnej wzajemnej interoperacyjności nowo dostarczanych i wdrażanych systemów z modułami/grupami/systemami funkcjonującymi u Zamawiającego. W przypadku wymiany systemu SSI na inny (innego producenta lub obecnego producenta, ale z innej linii produktowej) Zamawiający wymaga aby zachowana została obecna pełna międzymodułowa wymiana danych z wszystkimi obecnymi systemami, integracja z wszystkimi obecnie podłączonymi urządzeniami oraz systemami zewnętrznymi, a także oczekuje przeprowadzenia instruktaży dla wszystkich użytkowników systemu w szpitalu.
2. Szpitalny System Informatyczny, stanowiący źródło Elektronicznej Dokumentacji Medycznej EDM musi mieć zaimplementowane i uruchomione mechanizmy integracji oraz zapewnić prawidłową integrację z systemem EDM,
3. W SSI należy zapewnić spełnienie przez ten system wymagań Web Content Accessibility Guidelines (WCAG 2.1), z uwzględnieniem poziomu AA, określonych w załączniku nr 4 do rozporządzenia.
4. **Zamawiający informuje, że posiada następujące systemu i urządzenie, które należy z oferowanym systemem:**

SYSTEMY				
Lp.	**Nazwa**	**wersja/TYP**	**Producent**	**Umowa serwisowa**
1.	**Centrum - Laboratorium**	**2.487.4.1578**	**Marcel S.A.**	**Brak**
2.	**DiaHem – Bank Krwi**	**8.14.1**	**Diahem Diagnostic Products**	**Jest aktualna**
3.	**ES Apteka Szpitalna**	**2.163.981**	**Eurosoft**	**Brak**
4.	**NETRAAD Pacs – System RIS**	**2.1**	**CGM**	**Jest aktualna**
URZĄDZENIA				
1	**Skaner RTG**	**MAX975**	**KODAK**	**Jest aktualna**
2	**Skaner RTG**	**Classic**	**KODAK**	**Jest aktualna**
3	**Tomograf**	**Siemens SOMATOM go.ALL**	**Siemens**	**Jest aktualna**
4	**Aparat RTG DR**	**Digital Diagnost C50**	**Philips**	**Brak**
5	**Aparat RTG mobilny DR**	**MobileArt Evolution MX-7**	**SHIMADZU**	**Jest aktualna**
6	**Duplikator**	**EPSON PP-100II**	**EPSON**	**Jest aktualna**
7	**Duplikator**	**Rimage 2000i**	**RIMAGE**	**Brak**
8	**Duplikator**	**Rimage 2000i**	**RIMAGE**	**Brak**
9	**TK siemens – serwer tomografu**	**HP E ProLiant ML 110**	**Hewlett Packard**	**Jest aktualna**
10	**Stacja Opisowa ogólnodiagnostyczna**	**Dell Precision T3500**	**DELL**	**Brak**
11	**Stacja Opisowa mammograficzna**	**Dell Precision T3500**	**DELL**	**Brak**

12	Stacja Przeglądowa - RADIANT	Dell Precision T7400	DELL	Brak
13	Stacja Przeglądowa - RADIANT	Dell Precision T7400	DELL	Brak
14	Stacja Przeglądowa - RADIANT	DELL OPTIPLEX 780	DELL	Brak
15	Stacja Przeglądowa - RADIANT	DELL OPTIPLEX 780	DELL	Brak
16	Aparat USG	Affiniti 50	Philips	Brak

5. **Zamawiający przestawia zakres wymiany danych:**

SYSTEMY				
Lp.	Nazwa	wersja/TYP	Producent	Protokół wymiany danych
1.	Centrum - Laboratorium	2.487.4.1578	Marcel S.A.	HL 7
2.	DiaHem – Bank Krwi	8.14.1	Diahem Diagnostic Products	HL 7
3.	ES Apteka Szpitalna	2.163.981	Eurosoft	HL 7
4.	NETRAAD Pacs – System RIS	2.1	CGM	HL 7 + DICOM
URZĄDZENIA				
1	Skaner RTG	MAX975 nr 5573	KODAK	DICOM
2	Skaner RTG	Classic	KODAK	DICOM
3	Tomograf	Siemens SOMATOM go.ALL	Siemens	DICOM
4	Aparat RTG DR	Digital Diagnost C50	Philips	DICOM
5	Aparat RTG mobilny DR	MobileArt Evolution MX-7	SHIMADZU	DICOM
6	Duplikator	EPSON PP-100II	EPSON	DICOM
7	Duplikator	Rimage 2000i	RIMAGE	DICOM
8	Duplikator	Rimage 2000i	RIMAGE	DICOM
9	TK siemens – serwer tomografu	HP E ProLiant ML 110	Hewlett Packard	DICOM
10	Stacja Opisowa ogólnodiagnostyczna	Dell Precision T3500	DELL	DICOM
11	Stacja Opisowa mammograficzna	Dell Precision T3500	DELL	DICOM
12	Stacja Przeglądowa - RADIANT	Dell Precision T7400	DELL	DICOM
13	Stacja Przeglądowa - RADIANT	Dell Precision T7400	DELL	DICOM
14	Stacja Przeglądowa - RADIANT	DELL OPTIPLEX 780	DELL	DICOM
15	Stacja Przeglądowa - RADIANT	DELL OPTIPLEX 780	DELL	DICOM
16	Aparat USG	Affiniti 50	Philips	DICOM

Kompletną dokumentację pełnego zakresu wymiany danych Zamawiający udostępni po rozstrzygnięciu przetargu wybranemu Wykonawcy.

6. **Zamawiający dopuszcza wymianę w przypadku, gdy zaproponowane rozwiązanie zapewni wszystkie funkcjonalności działające obecnie w środowisku Zamawiającego, wskazane w Załączniku nr 1A do SIWZ. W przypadku braku jakiejkolwiek ze wskazanych funkcjonalności Zamawia-**

jący będzie miał prawo do odstąpienia od umowy z winy Wykonawcy oraz naliczenia kar umownych zgodnie z Dodatkiem nr 4 do SIWZ. Wykonawca poświadcza powyższe składając oświadczenie zgodnie z Dodatkiem nr 11 do SIWZ.

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.

7. W przypadku wymiany systemu SSI, Wykonawca pokrywa wszelkie koszty związane z wymianą systemy, w tym koszty wymiany posiadanej infrastruktury informatycznej (jednostki komputerowe, systemu operacyjne) wykorzystywanej do pracy w systemie SSI przez pracowników Zamawiającego, w przypadku braku możliwości pracy posiadanej infrastruktury na zaproponowanym rozwiązaniu.

Zamawiający w poniższych tabelach przedstawia posiadaną infrastrukturę informatyczną wykorzystywaną do pracy z obecnie posiadanym systemem, z którym proponowane rozwiązanie będzie musiało współpracować:

Tabela 1
Jednostki komputerowe w podziale na system operacyjny

	Nazwa systemu operacyjnego	Ilość
1	MS Windows XP	8
2	MS Windows Vista	2
3	MS Windows 7	153
4	MS Windows 8	1
5	MS Windows 8.1	2
6	MS Windows 10	75
7	Terminal	28

Tabela 2
Ilość komputerów z niskim parametrem CPU oraz RAM w podziale na System Operacyjny

LP	CPU < Intel I3 < AMD Ryzen 3 Ilość	OS	RAM <= 4 GB Ilość
1	8	MS Windows XP	8
2	2	MS Windows Vista	2
3	56	MS Windows 7	82
4	0	MS Windows 8	1
5	2	MS Windows 8.1	2
6	13	MS Windows 10	16

Pozostałe jednostki komputerowe nie ujęte w tabeli 2, spełniają parametry CPU > Intel i3/ AMD Ryzen 3 oraz RAM > 4GB.

II.3.2 Dostępność dostarczanego rozwiązania

Szpitalny System Informatyczny SSI działa w trybie 24 godzinnym przez wszystkie dni w roku z dostępnością co najmniej na poziomie 99% w skali miesiąca dla części białej HIS oraz e-usług. System nie jest dostępny, gdy występuje sytuacja uniemożliwiająca wykorzystanie którejś z jego funkcji z przyczyn leżących wewnątrz Systemu (np. awarii, spadku przepustowości Systemu i wynikającego stąd przeciążenia Systemu). Planowane prace (tzw. down time) odbywają się w godzinach od 2:00 do 5:00. 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).

II.3.3 Wymagany stan docelowy

Zamawiający oczekuje dostarczenia i wdrożenia licencji Szpitalnego Systemu Informatycznego dla nw. modułów:

Zakres dostawy i wdrożenia oprogramowania

LP.	MODUŁ	ILOŚĆ LICENCJI (SZT.) DOCELOWA NA MODUŁ
Moduły HIS		
1.	EDM	1
2.	Powiadomienia	1
3.	Konsultacje	1
4.	Wywiad	1
eUsługi		
1.	System kolejkowy wraz z niezbędnym sprzętem komputerowym	1
2.	eWyniki	1
Migracja na nową bazę danych		1

Oferowane produkty w ramach SSI muszą posiadać i realizować co najmniej funkcjonalności przedstawione w rozdziale II.3.5 SOPZ.

W chwili obecnej Zamawiający użytkuje Szpitalny System Informatyczny w części „szarej” system firmy HEX, a w części „białej” HIS system Clinninet firmy CompuGroupMedical.

Lp.	Moduły	Nazwa systemu	Ilość*
1.	JPK	CGMCLININET	1
2.	Oddział	CGMCLININET	1
3.	Poradnia	CGMCLININET	1
4.	Diagnostyka	CGMCLININET	1
5.	Blok Operacyjny	CGMCLININET	1
6.	Izba Przyjęć	CGMCLININET	1
7.	SIK	CGMCLININET	1
8.	Recepcja	CGMCLININET	1
9.	Umowy	CGMCLININET	1
10.	Statystyka	CGMCLININET	1
11.	Konfiguracja	CGMCLININET	1
12.	STER	CGMCLININET	1
13.	eRejestracja	CGMCLININET	1
14.	SASBI	CGMCLININET	1

II.3.4 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.
2. Zamawiający wymaga w zakresie dostarczonego rozwiązania informatycznego, 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 co najmniej takimi jak:
    a) Słownik ICD 9 i ICD 10,
    b) Słownik Instytucji właściwych UE,
    c) Miejscowości i kody terytorialne,
    d) Inne które zostaną ustalone z Zamawiającym w ramach analizy przedwdrożeniowej.

5. W przypadku wymiany SSI na inny system Zamawiający oczekuje przeniesienia wszystkich danych zgromadzonych dotychczas w systemie do nowego SSI. W Systemie muszą być zaimplementowane mechanizmy walidacji haseł zgodnie z wymaganiami ustawowymi przewidzianymi dla rodzaju danych przetwarzanych przez System.
6. System musi być dostosowany do struktury organizacyjnej Zamawiającego.
7. 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.
8. 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.

9. System musi mieć możliwość definiowania listy personelu białego (w szczególności lekarzy, pielęgniarek, położnych, techników) i ich specjalności zgodnie ze słownikiem i wymaganiami NFZ.
10. System musi być zintegrowany, przez co rozumie się zintegrowaną pracę wszystkich systemów/modułów w oparciu o swobodną, automatyczną wymienialność danych pomiędzy elementami (modułami) systemu.
11. System musi pozwalać na obsługę zdarzeń niepożądanych w określonym przedziale czasowym, nadawanie dostępu do funkcjonalności zgodnie z nadanymi uprawnieniami.
12. **System musi być dostosowany do Zintegrowanego Systemu Zarządzania funkcjonującego obecnie w SPZZOZ w Staszowie opartego o wymagania standardów akredytacyjnych Ministra Zdrowia oraz wymagania norm ISO obowiązujących w SPZZOZ w Staszowie oraz Wykonawca zobowiązuje się na bieżąco dokonywać wszelkich zmian w oparciu o obowiązujące przepisy prawne. Wykaz posiadanych formularzy, raportów, wydruków oraz danych opisowych w Załączniku 1C.**
13. 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.
14. 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.

II.3.5 Szpitalny System Informatyczny – wymagania szczegółowe

Dostawa i wdrożenie SSI, ma obejmować dostawę odpowiednich licencji Szpitalnego Systemu Informatycznego, o funkcjonalnościach i na warunkach nie mniejszych niż opisane poniżej.

	E-WYNIKI
5.	Aplikacja umożliwia przeglądanie wyników badań i obrazów diagnostycznych w formacie DICOM/JPG przez pacjenta metodą zdalną za pośrednictwem Internetu.
10.	Pacjent korzystając z przygotowanej witryny internetowej może się zalogować, wybrać na podstawie różnych kryteriów (jednostka wykonująca, nazwa badania, status) interesujące go wyniki odczytać, pobrać lub wydrukować.
15.	Wyniki mogą być prezentowane jako lista lub hierarchicznie z podziałem na jednostki wykonujące.
20.	Możliwość prezentowania wyników badań tylko i wyłącznie skonsultowanych podczas porady pacjenta.
25.	Możliwość konfiguracji okresu widoczności danego wyniku na liście wyników pacjenta.
30.	Pełna integracja z Elektronicznym Rekordem Medycznym Pacjenta systemu szpitalnego, korzystanie z tego samego źródła danych, wspólnego modułu administracyjnego oraz słowników.
35.	Pacjent ma możliwość załączenia zeskanowanych załączników. Lekarz po stronie systemu medycznego HIS działającego w intranecie może zdecydować które z załączników dołączyć do dokumentacji medycznej wizyty.
	E-POWIADOMIENIA
5.	Moduł automatycznych powiadomień pacjenta o zbliżających się terminach wizyt oraz innych zdarzeń medycznych (np. termin badania, wizyty, informacje o badaniach profilaktycznych) za pomocą 3 kanałów komunikacji: e-mail, wiadomości systemowe portalu pacjenta dostępne po zalogowaniu do portalu e-Usług, opcjonalnie SMS za pomocą bramki SMS udostępnionej przez Zamawiającego.

10.	Generowanie wiadomości przypominających pacjentom o wizytach i badaniach.
15.	Wiadomości generowane są w pakietach.
20.	Możliwość konfiguracji formatu treści wiadomości do wysyłki, a w tym użycie parametrów: - imię pacjenta, - nazwisko pacjenta, - numer pacjenta, - data wizyty (dd-mm-yyyy), - dzień wizyty (dd), - miesiąc wizyty (numer w formacie mm lub słownie), - rok wizyty (yyyy), - godzina wizyty (HH:mm), - nazwa krótka usługi.
25.	Możliwość definicji szablonów wiadomości niezależnych dla każdego typu usług/porad.
30.	Możliwość definicji domyślnego szablonu wiadomości dla usług/porad/wizyt.
35.	Obsługa formatu co najmniej CSV dla pakietu dostarczanego dostawcy bramki SMS .
40.	Możliwość generowania wiadomości tylko dla pacjentów, którzy wyrazili zgodę na otrzymywanie komunikatów SMS.
45.	Wszystkie wysłane wiadomości są gromadzone w bazie danych systemu wraz z datą wygenerowania i są powiązane z wizytą, usługą, pacjentem, wykorzystanym szablonem wiadomości.
50.	Zabezpieczenie przed ponowną wysyłką tego samego komunikatu.
55.	Możliwość konfiguracji godziny oraz cykli w dniach, w jakich pakiety wiadomości będą generowane do wysyłki.
60.	Moduł komunikacji SMS jest zintegrowany z rejestrem wizyt i pacjentów systemu Ruchu Chorych.
65.	Możliwość konfiguracji maksymalnej długości wiadomości SMS.
70.	Automatyczna weryfikacja i generowanie wiadomości tylko do pacjentów posiadających uzupełniony w systemie numer telefonu komórkowego.
75.	Pacjent może wskazać jakie kanały komunikacji preferuje w przypadku powiadomień o wizytach, badaniach, zbliżającym się terminie przyjęcia do szpitala wg kolejki oczekujących, informacjach o badaniach profilaktycznych.
	e-Wywiad
2.	Moduł umożliwia pacjentowi przekazać lekarzowi istotne informacje przed wizytą.

4.	Moduł umożliwia skorzystanie ze zdefiniowanych formularzy strukturyzowanych, stworzonych w module Generator formularzy.
6.	Wprowadzony przez pacjenta e-Wywiad prezentowany jest w module gabinet lekarski.
8.	Lekarz ma możliwość zapoznania się z e-wywiadem przed wizytą. System umożliwia poinformowanie lekarza o uzupełnieniu przez pacjenta e-wywiadu. Lekarz ma możliwość zadania dodatkowego pytania pacjentowi.
	E-KONSULTACJE Z PACJENTEM
5.	Moduł umożliwia konsultacje pisemne, gromadzone w powiązaniu z rekordem medycznym pacjenta między lekarzem a pacjentem. Umożliwia zadawanie pytań / zgłaszanie uwag przez pacjentów poprzez wewnętrzny system komunikacji.
10.	W części szpitalnej i poradni użytkownicy korzystają z wbudowanego w system do komunikacji z pacjentem.
15.	Pacjent może zwęzić konsultacje do wybranej poradni i lekarza na podstawie odbytych wizyt.
20.	Wiadomość wysłana z portalu przez zalogowanego pacjenta będzie dostępna w systemie HIS dla osoby podanej w konfiguracji funkcjonalności.
25.	Do wiadomości wysłanej przez pacjenta możliwa będzie generacja jednej odpowiedzi (dostępnej następnie do podglądu przez pacjenta na portalu).
30.	Pacjent zostanie poinformowany za pomocą maila o odpowiedzi na pytanie.
35.	Pacjent będzie miał dostęp do historii konsultacji pisemnych.
	REPOZYTORIUM ELEKTRONICZNEJ DOKUMENTACJI MEDYCZNEJ
4.	System musi umożliwiać wymianę dokumentacji medycznej między jednostkami ochrony zdrowia.
8.	Wymiana dokumentacji realizowana musi być poprzez elektroniczną wymianę komunikatów między systemami informatycznymi.
12.	System musi umożliwiać integrację między systemami medycznymi klasy HIS, AIS, LAB, RIS dowolnych producentów.
16.	System musi umożliwiać wymianę dokumentów medycznych w dowolnym formacie, w szczególności PDF, DOC, RTF, HL7 CDA.
20.	System musi umożliwiać przekazywanie wyników badań obrazowych w formacie DICOM.
24.	System musi posiadać zaimplementowane dokumenty medyczne zgodne ze standardem HL7 CDA opisanym przez CSIOZ na stronie Polska Implementacja HL7 CDA (https: //www.csioz.gov.pl/HL7POL/pl-cda-html-pl-PL/)
28.	Wymiana dokumentacji realizowana musi być w oparciu o otwarte, międzynarodowe standardy IHE XDS.

32.	Komunikacja między placówkami musi odbywać się za pomocą sieci Internet.
36.	Przesyłane dane muszą być szyfrowane i podpisywane podpisem elektronicznym.
40.	Podłączenie systemu zewnętrznego realizowane musi być za pomocą protokołu IHE XDS
44.	System musi posiadać wsparcie dla protokołu HL7 v3 w zakresie: 1) parsowanie i generowanie komunikatów, 2) walidacja komunikatów, 3) rejestr OID - generowanie wrapperów HL7 (ControlActWrapper i TransmisionWrapper) - generowanie potwierdzeń Ack.
48.	System musi posiadać wsparcie dla protokołu DICOM
52.	Dostęp do aplikacji musi być zabezpieczony loginem i hasłem
56.	Użytkownicy muszą być uwierzytelniani za pomocą: 1) lokalnej bazy danych użytkowników, 2) baz danych użytkowników podłączonych systemów, 3) lokalnego repozytorium LDAP, 4) zdalnych repozytoriów LDAP.
60.	System musi umożliwiać pobranie dokumentacji medycznej wybranego pacjenta.
64.	Repozytorium musi obsługiwać profil integracyjny IHE XDS.b.
68.	Dokumenty umieszczone w Repozytorium EDM nie mogą być zmieniane ani usuwane przed upływem okresu retencji. Repozytorium musi umożliwiać wykonywanie adnotacji do dokumentów oraz dodawanie kolejnych wersji dokumentu. Repozytorium musi przechowywać zarówno dokument oryginalny oraz wszystkie ewentualne wersje dokumentu. Repozytorium musi przechowywać relacje pomiędzy dokumentem oryginalnymi i jego kolejnymi wersjami.
72.	Repozytorium musi przechowywać informacje o zgodach na udostępnienie dokumentacji medycznej.
76.	Repozytorium musi mieć możliwość przechowywania informacji o miejscu składowania dokumentu fizycznego.
80.	Dokumenty przechowywane w Repozytorium mogą być podzielone na typy. Typ dokumentu musi być opisywany za pomocą zestawu metadanych. Metadane dla każdego z typów muszą być wymagane lub opcjonalne.

84.	Każdy dokument przechowywany w repozytorium musi być opatrzony, co najmniej następującymi metadanymi: 1) unikalny identyfikator dokumentu, 2) identyfikator pacjenta (dla dokumentacji indywidualnej), 3) identyfikator jednostki (dla dokumentacji zbiorczej), 4) data utworzenia dokumentu, 5) data wprowadzenia dokumentu do repozytorium, 6) nazwa i typ dokumentu, 7) rodzaj i nazwa jednostki medycznej, w której dokument został wytworzony, 8) status dokumentu (aktualny, nie aktualny), 9) kategoria archiwalna/okres retencji dokumentu.
88.	Repozytorium musi umożliwiać brakowanie dokumentów po upływie okresu retencji.
92.	Repozytorium musi przechowywać informacje o udostępnieniu dokumentu, co najmniej przez okres retencji dokumentu.
96.	Repozytorium musi przechowywać wszystkie dane związane z żądaniem udostępnienia dokument, bez względu na rezultat żądania (udostępnienie/odmowa dostępu).
100.	Repozytorium musi weryfikować metadane rejestrowanego dokumentu.

MODUŁ OBSŁUGI KOLEJKI - INFOKIOSK	
1	Moduł umożliwia generowanie numerów do obsługi kolejki i pobranie numeru z infokiosku przez pacjenta.
2	Moduł umożliwia weryfikację zapisanych w systemie medycznym danych pacjenta umówionego na wizytę: terminu wizyty; weryfikacji czy umówiona wizyta posiada uzupełnione skierowanie oraz weryfikacji uprawnień pacjenta (czy pacjent posiada uzupełnione aktualne ubezpieczenie).
3	Moduł umożliwia potwierdzenie wizyty w umówionym dniu poprzez aktywację usługi na infokiosku. Potwierdzenie może nastąpić po wpisaniu danych pacjenta uzupełnionych w systemie medycznym: numeru PESEL
4	Moduł umożliwia pacjentowi pobranie numeru do punktu rejestracji wizyt (numer nie powiązany z danymi pacjenta).
5	Drukarka infokiosku powinna wydrukować numer identyfikacyjny dla zarejestrowanej wizyty oraz dodatkowe informacje na papierze (imię i nazwisko lekarza, numer gabinetu, **ilością osób oczekujących w kolejce, nazwą kolejki, do której bilet został wydrukowany oraz szacowany czas oczekiwania na wezwanie).**

6	Moduł umożliwia potwierdzenie wizyty pacjenta przez personel przychodni bezpośrednio w module rejestracji wizyt. Wprowadzenie pacjenta do kolejki po weryfikacji lub uzupełnieniu brakujących danych w systemie medycznym (dane skierowania, informacje o ubezpieczeniu). Personel przychodni może wygenerować numer identyfikacyjny dla wizyty. Numer identyfikacyjny wizyty może być umieszczony na wydruku generowanym z systemu.
7	Możliwość wyświetlania kolejki pacjentów oczekujących na wyświetlaczach zbiorczych w poczekalni (zgodnie z przepisami – ukrywając dane osobowe, np. numer generowany z infokiosku).
	MODUŁ OBSŁUGI KOLEJEK - ADMINISTRACJA
1	Uwierzytelnienie i autoryzacja dostępu do modułu.
2	Zarządzanie użytkownikami modułu wspólne z zarządzaniem użytkownikami systemu medycznego np.: z wykorzystaniem AD.
3	Możliwość konfiguracji kolejek - przypisanie kodu, opisu i jednostki organizacyjnej w systemie (dodawanie, usuwanie).
4	Możliwość definiowania kolejek związanych z punktem rejestracji wizyt.
5	Możliwość konfiguracji widoku danych na monitorach LCD - wybór kolejek wyświetlanych na poszczególnych monitorach, możliwość konfiguracji widoku kolejki (układ tabelaryczny / pojedyncza kolejka). -– **dodatkowo punktowane w kryterium oceny ofert**
6	Interfejs systemu w języku polskim
7	Moduł obsługi kolejek działa w oparciu o architekturę klient – serwer i jest uruchamiany automatycznie podczas włączania serwera.
8	Obsługa powiadomień. W tym: systemowych (informacja o końcu papieru w Infokiosku, wyłączenie się danego urządzenia, nowy numer w kolejce). Możliwość włączania / wyłączania poszczególnych typów powiadomień.
9	Moduł archiwum numerów z funkcją wyszukiwarki numeru po parametrach (numer, nazwa biletu, status, kolejka, pomieszczenie)
10	Realizacja funkcji cyfrowy bilet, poprzez prezentację w telefonie pacjenta informacji i realizację usług dotyczących jego wizyty w tym: • pobranym wirtualnym numerze kolejkowym przez pacjenta • lokalizacji wizyty (numer pomieszczenia, piętro) • personalia lekarza prowadzącego • aktualnej pozycji na liście oczekujących - informacja aktualizowana na bieżąco • powiadomienia o (jesteś pierwszy na liście, wezwanie do gabinetu)

11	Wyświetlanie komunikatów (wbudowany edytor tekstu) na monitorach w formie paska informacyjnego na dole ekranu. Możliwość wskazania wybranych monitorów na które można wysłać komunikat. oraz ustalenia harmonogramu prezentacji
12	Wyświetlanie komunikatów RSS na monitorach w formie paska informacyjnego na dole ekranu. Możliwość wskazania wybranych monitorów na które można wysłać komunikat oraz ustalenia harmonogramu prezentacji
13	Wprowadzenie ogłoszeń w formacie plików graficznych lub video (JPG, PNG, MP4) wyświetlanych na monitorach. System udostępnia wyświetlanie tych ogłoszeń równocześnie z prezentacją kolejek tzn. możliwość wyświetlania widoku aplikacji (w tym: widok kolejek, przywołanie pacjenta) i ogłoszeń na przemian w określonej sekwencji czasowej. Podczas prezentacji ogłoszeń aplikacja na monitorze umożliwia prezentację okna wywołania numeru pacjenta (komunikaty wywołania pacjenta mają priorytet przed ogłoszeniami).
MODUŁ OBSŁUGI KOLEJKI - PRZYWOŁANIE PACJENTA DO GABINETU LEKARSKIEGO	
1	Moduł dostępny jest dla użytkowników w module gabinetowym.
2	Moduł umożliwia użytkownikowi wybór zdefiniowanej wcześniej kolejki, z którą będzie pracował.
3	Moduł umożliwia przywołanie do gabinetu lekarskiego pacjenta, który potwierdził swoje przybycie na wizytę w infokiosku lub rejestracji.
4	Użytkownik moduł gabinetowego ma dostęp do listy pacjentów, którzy potwierdzili przybycie na wizytę.
5	Przywołanie pacjenta do gabinetu lekarskiego - automatycznie otwiera ekran wizyty pacjenta w module gabinetowym. – **dodatkowo punktowane w kryterium oceny ofert**
6	Przywołanie pacjenta do gabinetu lekarskiego przez użytkownika w gabinecie powoduje wyświetlenie informacji na monitorze w poczekalni. - – **dodatkowo punktowane w kryterium oceny ofert**
7	Moduł prezentuje liczbę osób aktualnie oczekujących na wizytę.
8	Moduł prezentuje użytkownikowi systemu imię i nazwisko osoby aktualnie wezwanej do gabinetu.
9	Moduł umożliwia ponowne przywołanie pacjenta do gabinetu.
10	Moduł umożliwia ponowne wstawienie pacjenta do kolejki przez użytkownika. – **dodatkowo punktowane w kryterium oceny ofert**
11	Moduł umożliwia dodanie pacjenta do kolejki przez użytkownika modułu w rejestracji.

12	Moduł w dowolnym momencie umożliwia użytkownikowi modułu gabinetowego przywołanie pacjenta poza kolejnością.
13	Moduł umożliwia generowanie komunikatów dźwiękowych na wskazanych monitorach w poczekalni w momencie, kiedy kolejny pacjent jest przywoływany do gabinetu.
14	Moduł umożliwia wprowadzenie przez użytkownika w gabinecie informacji o rozpoczęciu /zakończeniu przerw - informacja o przerwie prezentowana jest na monitorach w poczekalni.
15	Moduł powiadamia o kolejce pacjentów oczekujących, na monitorach w poczekalni lub innych wskazanych miejscach instalacji monitorów objętych systemem kolejkowym. Monitory przygabinetowe wyświetlają m.in. informacje o numerze wywoływanego biletu oraz nazwy poradni, numer gabinetu, personalia lekarza przyjmującego w danym gabinecie, numery oczekujące do gabinetu.
MODUŁ OBSŁUGI KOLEJKI - PRZYWOŁANIE PACJENTA DO REJESTRACJI	
1	Moduł dostępny jest dla użytkownika w module rejestracji wizyt pacjentów.
2	Moduł umożliwia użytkownikowi wybór zdefiniowanej wcześniej kolejki, z którą będzie pracował.
3	Moduł umożliwia przywołanie pacjenta do rejestracji.
4	Moduł umożliwia połączenie numeru pobranego przez pacjenta w infokiosku z zarejestrowaną wizytą - tak aby nie było konieczności nadawania kolejnego numeru dla pacjenta. – **dodatkowo punktowane w kryterium oceny ofert**
5	Przywołanie pacjenta do punktu rejestracji wizyt powoduje wyświetlenie informacji na monitorze w poczekalni.
6	Moduł umożliwia ponowne przywołanie pacjenta do punktu rejestracji.
OBSŁUGA POTWIERDZEŃ	
1	Integracja Systemu z systemem szpitalnym HIS w zakresie pobrania danych pacjenta umówionego na wizytę.
2	Potwierdzenie wizyty w umówionym terminie przez aktywację usługi na Infokiosku. Potwierdzenie może nastąpić po wpisaniu numeru PESEL lub zeskanowaniu kodu kreskowego z dokumentu potwierdzenia rejestracji. W przypadku konieczności uzupełnienia dokumentacji medycznej (brak skierowania, brak ubezpieczenia) pacjent dostaje informację o konieczności zgłoszenia się do Rejestracji Poradni.
3	Po wprowadzeniu numeru PESEL lub zeskanowaniu kodu kreskowego i uzyskaniu informacji o potwierdzeniu drukarka Infokiosku powinna wydrukować informacje (w tym nazwę kolejki/poradni, numer gabinetu, **imię i nazwisko lekarza, ilością osób oczekujących w kolejce, nazwą kolejki, do której bilet został wydrukowany oraz szacowany czas**

	oczekiwania na wezwanie).
4	System powinien mieć funkcję potwierdzenia wizyty pacjenta przez personel przychodni (opcjonalnie — jeżeli nie chcemy by Pacjent sam potwierdzał swoje przybycie). Wprowadzenie pacjenta do kolejki oczekujących przez weryfikacje danych (np. numer PESEL).
5	System musi prezentować użytkownikom systemu listę pacjentów z potwierdzoną wizytą do właściwych kolejek. Listy pacjentów są widoczne dla uprawnionych użytkowników

WYŚWIETLACZ GABINETOWY 21” – 20 SZTUK /WYŚWIETLACZ REJESTRACJA 21’’– 5 SZTUK	
MINIMALNE PARAMETRY TECHNICZNE	
Monitor	• rozdzielczość min: 1920x1080 px • panel: LED/LCD • rozmiar min. 21,5” • jasność min: 250cd/m2 • kontrast min: 1000;1 • głośniki 2 x min. 1,5W • procesor o taktowaniu min 1,5 Ghz • pamięć min: 2 GB RAM • dysk twardy lub eMMC min: 8GB • porty min. 2 x USB • komunikacja: 1x LAN, Wi-Fi
Mocowanie	• uchwyt umożliwiający trwałe zamocowanie do ściany lub sufitu monitora
Uwagi	• Monitor przewidziany do pracy ciągłej 24/7

WYŚWIETLACZ ZBIORCZY 50’’ – 1 SZTUKA	
MINIMALNE PARAMETRY TECHNICZNE	
Monitor	• rozdzielczość min: 1920x1080 px • rozmiar min. 49” • panel LED/LCD • jasność: min. 350 cd/m2 • kąty widzenia obrazu: 178 / 178 • głośniki wbudowane 2 x min. 6 W • procesor o taktowaniu min 1,5 Ghz • pamięć min: 2 GB RAM

	• dysk twardy lub eMMC min: 8GB • porty min. 2 x USB, 1x audio in, 1x audio out • komunikacja : 1x LAN, Wi-Fi
Mocowanie	• uchwyt umożliwiający trwałe zamocowanie do ściany lub sufitu monitora
Uwagi	• Monitor przewidziany do pracy ciągłej

DRUKARKA BILETÓW BIURKOWA – 1 SZT.	
MINIMALNE PARAMETRY TECHNICZNE	
Parametry wydruku	• metoda druku: termiczna • prędkość: max 250mm/s • rozdzielczość: 203 DPI
Papier	• typ papieru: termiczny • szerokości 57,80mm
Wytrzymałość	• 100 mln pulsów lub więcej 150km lub więcej 2mln ucięć
Kody kreskowe	• upc-a, upc-e, ean8, ean13, code39, itf, codebar, code128, code93, pd417, qr code
Interfejsy komunikacyjne	• USB, Ethernet
Obudowa	• Obudowa zapobiegającą zachlapaniu oraz zakurzeniu wnętrza drukarki

Infokioski/Automaty biletowe stojące zostaną zainstalowane przy wejściu do placówki, aby zapewnić wszystkim pacjentom możliwość wygodnego pobrania biletu i zarejestrowania się w systemie. Za pomocą dotykowego ekranu pacjent definiuje cel swojej wizyty. Na podstawie wprowadzonych danych zostanie wydrukowany bilet kolejkowy.

Zamawiający **nie zapewni** we własnym zakresie dostępność gniazd prądowych oraz sieciowych. **W celu poprawnego działania oraz możliwości egzekwowania warunków gwarancji Wykonawca zobowiązany jest wykonać fizyczny montaż dostarczonego sprzętu wraz z wykonaniem podłączeń elektrycznych i sieciowych. Plany budynków wraz z opisem przebiegu tras kablowych i podłączeń elektrycznych stanowi załącznik nr 1D do SIWZ.**

Jednocześnie Zamawiający umożliwi Wykonawcy przeprowadzenie wizji lokalnej w miejscu instalacji Infokiosków/ automatów biletowych oraz wszystkich urządzeń niezbędnych do działania systemu kolejkowego. 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 komórki właściwej ds. Informatyki, dostępny pod nr tel. 15 864 85 00.

INFOKIOSK WOLNOSTOJĄCY – 2 SZTUKI	
ELEMENT	**OPIS MINIMALNYCH PARAMETRÓW TECHNICZNYCH**
Obudowa	• konstrukcja wykonana z blachy stalowej, o konstrukcji samonośnej zapewniającej sztywność obudowy • montaż monitora w obudowie w orientacji pionowej • wolnostojąca, uniemożliwiająca dostęp z zewnątrz do podzespołów wewnętrznych i jakichkolwiek połączeń, dostęp serwisowy poprzez drzwiczki rewizyjne z zamkiem patentowym • na froncie obudowy logo lub grafika zgodna z wymaganiami placówki • obudowa pomalowana farbą antybakteryjną w kolorystyce ustalonej z Zamawiającym
Monitor	· przekątna monitora min 21” · rodzaj wyświetlacza: pojemnościowy Edge LED · kąt widzenia obrazu (poziom/pion) min: 178 poziomo / 178 pionowo · naturalna rozdzielczość pracy min: 1920 x 1080 · Jasność min. 350 cd/m2 · Kontroler dotyku Projected Capacitive Technology (PCT), Liczba punktów dotyku 10 · Przystosowany do pracy 24/7 · Powłoka antybakteryjna
Jednostka sterująca	· procesor min. 2 rdzeniowy o taktowaniu min, 1,6 Ghz · pamięć min: 4 GB RAM · dysk twardy SSD min:120GB · min 2 x USB · min 1x HDMI
Drukarka biletów	• Metoda druku: termiczny druk liniowy • Komunikacja – USB, • Rozdzielczość:203 dpi • Szerokość papieru: 58/60/80mm • Maksymalna szybkość druku: 200 mm/s • Grubość papieru termoczułego: 65 do 150 µm • Automatyczne ucinanie: pełne oraz częściowe • Zestaw znaków:

	PC437/850/852/857/858/860/863/865/866/1250,WPC1252
Czytnik kodów kreskowych	· Odczyt kodów 1D (jednowymiarowych) · Odczyt kodów 2D (dwuwymiarowych np. kody QR)

II.3.6 Dane w systemie HIS

Zamawiający oświadcza, że posiada oprogramowanie dedykowane do pracy w środowisku Szpitala - CGM CLININET. Zamawiający nabył oprogramowanie, które użytkuje na podstawie innych postępowań publicznych i nie posiada do niego odmiennych praw licencyjnych związanych z prawami autorskimi zgodnie z art. 52 ust 1 Ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tj. Dz. U. z 2019 r. poz. 1231.) zwaną dalej Papp. Zamawiający na podstawie swojej licencji do posiadanego oprogramowania, ma prawo do m.in. zwielokrotniania kodu lub tłumaczenie jego formy w rozumieniu art. 74 ust. 4 pkt 1 i 2 Papp, jeżeli jest to niezbędne do uzyskania informacji koniecznych do osiągnięcia współdziałania niezależnie stworzonego programu komputerowego z innymi programami komputerowymi, o ile zostaną spełnione następujące warunki:

a) czynności te dokonywane są przez licencjobiorcę lub inną osobę uprawnioną do korzystania z egzemplarza programu komputerowego bądź przez inną osobę działającą na ich rzecz,
b) informacje niezbędne do osiągnięcia współdziałania nie były uprzednio łatwo dostępne dla osób, o których mowa pod lit. a,
c) czynności te odnoszą się do tych części oryginalnego programu.

Ponadto, oprogramowanie, które Zamawiający używa, korzysta z bazy danych, która nosi znamiona i cechy utworu zgodnie z art. 1 Papp oraz podlega ochronie sui generis zgodnie z definicją bazy danych zawartą w ustawie z dnia 27 lipca 2001 roku o ochronie baz danych (tj. Dz. U. 2018 r. poz. 2339.), dalej Obd.

Dane zawarte w tej bazie danych są danymi Zamawiającego, jednak w momencie tworzenia bazy danych systemu użytkowanego przez Zamawiającego, dane te w momencie migracji i wprowadzania danych do systemu, zostały usystematyzowane, uporządkowane według określonych paramentów, narzuconych przez uprzedniego wykonawcę, a przez to stały się częścią składową tej bazy danych, w zgodzie z art. 2 ust. 1 pkt. 1 Obd. Wykonawca, może pobrać dane z bazy danych tylko i wyłącznie na podstawie przepisów ustawy, w szczególności art. 2 ust. 1, art. 7 oraz art. 8 ust. 2 Obd. Zamawiający może pobrać jedynie dane określone poniżej i przekazać je Wykonawcy w postaci uporządkowanych plików xls lub txt.

Wykonawca jest zobowiązany do dostarczenia w nowym środowisku wszystkich funkcjonalności systemu posiadanego przez Zamawiającego w następujących obszarach:

1. System po przeprowadzonym procesie migracji musi zachować pełną funkcjonalność użytkowaną obecnie przez Zamawiającego.

2. System po przeniesieniu danych na nową bazę danych ma zachować możliwość użytkowania wszystkich raportów, wydruków oraz formularzy używanych obecnie przez Zamawiającego. Wykonawca w ramach etapu analizy przedwdrożeniowej wykona inwentaryzację tych elementów. Wykonawca ma obowiązek przeniesienia wszystkich tych elementów w ramach procesu migracji.
3. System musi być uruchomiony i wdrożony we wszystkich komórkach organizacyjnych Zamawiającego.
4. System musi mieć możliwość zachowania ciągłości pracy wszystkich użytkowników. Jeżeli elementy interfejsu graficznego systemu i/lub przebiegu procesu ulegną zmianie w wyniku przenoszenia danych Wykonawca jest zobowiązany w tych obszarach przeszkolić wszystkich użytkowników systemu. Wymagania dla procesu szkoleń przedstawione są w pkt. Instruktaże.
5. Wykonawca jest zobowiązany do uruchomienia pełnego zakresu integracji z systemami Zamawiającego. Koszt ewentualnej modyfikacji integrowanych systemów stanowi koszt Wykonawcy i jest on w pełni odpowiedzialny za uruchomienie pełnych funkcjonalności integracji po wykonaniu migracji w momencie startu produkcyjnego systemu po migracji.
6. Wykonawca jest zobowiązany do skonfigurowania procedur backupu systemu z wykorzystaniem narzędzi używanych przez Zamawiającego.

II.3.7 Interfejsy komunikacyjne

Zamawiający wymaga aby w zakresie nowo wdrażanych systemów objętym niniejszym zamówieniem, Wykonawca przedstawił stosowny dokument, opisujący „Interfejs komunikacyjny API systemu szpitalnego Zamawiającego do systemów EDM i e-Usług" z systemami programowymi Wykonawcy, pozwalający na integrację bazy danych systemu z innymi systemami, będącymi w przyszłości instalowanymi w infrastrukturze Zamawiającego, oraz opis struktury bazy danych systemu, tak aby w przyszłości w trakcie jego wymiany, można było bezproblemowo migrować dane zamawiającego, które w momencie wdrożenia systemu zostały ustandaryzowane.

Zamawiający do przeprowadzenia procesu przenoszenia danych bazy danych udostępni interfejs administracyjny serwerów baz danych w trybie odczytu. Wykonawca nie może ingerować w dane ani strukturę danych jak i samych baz danych w celu przeprowadzenia procesu migracji danych.

II.3.8 Baza DANYCH

Wykonawca wykona wszystkie prace programistyczne i migracyjne związane z zasileniem danymi w celu przeniesienia wszystkich funkcjonalności obecnie funkcjonującego systemu HIS Zamawiającego, którym jest obecnie system CompuGroup Medical Polska CLININET Sybase, na nowy wydajniejszy silnik bazodanowy w szybkim środowisku bazodanowym, który Wykonawca dostarczy i zainstaluje zgodnie z rozdziałem II niniejszego zamówienia. Lista funkcjonalności systemu CLININET opartego o aktualną bazę danych stanowi Załącznik nr 1A do SIWZ. Wykonawca musi odtworzyć wszystkie funkcjonalności zawarte w tym załączniku na nowym środowisku bazodanowym, instalując system HIS w nowym środowisku

bazodanowym. Wszystkie odtwarzane funkcjonalności systemu na nowej bazie danych muszą zostać szczegółowo odwzorowane zgodnie z załącznikiem dotyczącym funkcjonalności i formularzy: Załącznik nr 1A do SIWZ - Lista funkcjonalności obecnie użytkowanego systemu HIS podlegającego przeniesieniu na nową bazę danych.

Dodatkowo Zamawiający wymaga, aby wszystkie dane zawarte w systemie HIS obecnie funkcjonującym, były przeniesione do nowej bazy danych systemu HIS na zasadach określonych w pkt OPZ – Migracja danych.

Zamawiający wymaga dostarczenia nowej, wydajnej bazy danych, które umożliwi również przeniesienie na dostarczone w niniejszym postępowaniu macierz i serwery.

Wymagane jest dostarczenie licencji bazodanowych umożliwiające uruchomienie na 2 fizycznych procesorach o poniższych wymaganiach minimalnych:

	WYMAGANIA MINIMALNE
1.	Licencje na motor bazy danych umożliwiające uruchomienie na 2 fizycznych procesorach klasy x86 (po 1 w 2 serwerach spiętych w klaster). Licencja musi być dożywotnia. Baza danych ma pracować na fizycznych serwerach. Baza danych musi być zgodna z aplikacją posiadaną przez Zamawiającego. Wymagane jest dostarczenie licencji wraz ze wsparciem na min. 1 rok.
2.	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.
3.	Dedykowana dla silnika baz danych platforma musi zapewnić jego produkcyjne wykorzystanie w zakresie wszystkich minimalnych parametrów technicznych.
4.	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.
5.	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.
6.	Wsparcie dla wielu ustawień narodowych i wielu zestawów znaków (włącznie z Unicode).
7.	Możliwość migracji zestawu znaków bazy danych do Unicode
8.	Możliwość redefiniowania przez Zamawiającego ustawień narodowych – symboli walut, formatu dat, porządku sortowania znaków za pomocą narzędzi graficznych.
9.	Skalowanie rozwiązań opartych o architekturę trójwarstwową: możliwość uruchomienia wielu sesji bazy danych przy wykorzystaniu jednego połączenia z serwera aplikacyjnego do serwera bazy danych
10.	Możliwość otworzenia wielu aktywnych zbiorów rezultatów (zapytań, instrukcji DML) w jednej sesji bazy.
11.	Wsparcie protokołu XA, Wsparcie standardu JDBC 3.0
12.	Zgodność ze standardem ANSI/ISO SQL 2003 lub nowszym.
13.	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.
14.	Brak formalnych ograniczeń na liczbę tabel i indeksów w bazie danych oraz na ich rozmiar (liczbę wierszy).
15.	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
16.	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).
17.	Możliwość kompilacji procedur składowanych w bazie do postaci kodu binarnego (biblioteki dzielonej)

18.	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).
19.	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
20.	Możliwość autoryzowania użytkowników bazy danych za pomocą rejestru użytkowników założonego w bazie danych bądź mechanizmu wewnętrznego w stosunku do bazy danych.
21.	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.
22.	Licencja bazy danych powinna być bezterminowa.
23.	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.

II.3.9 Zakres i przedmiot zasilenia danymi bazę danych

Przedmiotem zamówienia jest także zasilenie funkcjonalności użytkowanego systemu CGM CLININET firmy CGM na wydajniejszy silnik bazy danych, celem podniesienia całkowitej wydajności i skalowalności systemu. Proces przenoszenia musi odbywać się ze szczególnym uwzględnieniem zachowania ciągłości pracy Zamawiającego i w ramach tego procesu wszelkie przestoje systemu muszą być zaplanowane i uzgodnione z Zamawiającym. W ramach procesu przenoszenia Wykonawca jest zobowiązany do przeniesienia danych z użytkowanych instancji (produkcyjnych i treningowych) systemu na nowy dostarczany w ramach zamówienia silnik bazy danych i uruchomienia w takiej konfiguracji wszystkich funkcjonalności systemu opisanych w Załączniku nr 1 do OPZ oraz uruchomienia systemu we wszystkich użytkowanych obecnie przez Zamawiającego aspektach to jest:

1. System musi być uruchomiony we wszystkich komórkach organizacyjnych Zamawiającego.

2. Musi mieć możliwość zachowania ciągłości pracy wszystkich użytkowników. Jeżeli elementy interfejsu graficznego systemu i/lub przebiegu procesu ulegną zmianie w wyniku migracji Wykonawca jest zobowiązany w tych obszarach przeszkolić wszystkich użytkowników systemu.
3. Wykonawca jest zobowiązany do uruchomienia pełnego zakresu integracji z systemami Zamawiającego. Koszt ewentualnej modyfikacji integrowanych systemów stanowi koszt Wykonawcy i jest on w pełni odpowiedzialny za uruchomienie pełnych funkcjonalności integracji po wykonaniu migracji.

W ramach procesu przenoszenia danych Wykonawca jest zobowiązany do wykonania następujących zadań:

1. Dostarczenia wydajnego silnika bazy danych przeznaczonego dla systemów HIS, wraz z usługą utrzymania i wsparcia zgodnie z Umową, którego wymagania opisane są w tym dokumencie we wskazanej liczbie licencji.
2. Wykonania audytu bieżącej instalacji systemu – wszystkich elementów systemu, celem określenia szczegółowej listy elementów niestandardowych, które będą podlegały odtworzeniu na nowym środowisku bazy danych w szczególności formularzy, raportów i wydruków używanych przez Zamawiającego.
3. Przedstawienia planu migracji i projektu technicznego migracji do akceptacji Zamawiającego.
4. Wykonania zaakceptowanego planu migracji w szczególności zainstalowania, uruchomienia i wdrożenia systemu na nowej wydajnej bazie danych wraz ze wszystkimi elementami niezbędnymi do jego poprawnego funkcjonowania takimi jak: systemy operacyjne, serwery aplikacyjne, konfiguracja bazy danych, itd.
5. Przeniesienia wszystkich danych z użytkowanego systemu CGM CLININET na nowy, wydajniejszy system zarządzania bazą danych (SZBD).
6. Wykonania wcześniej przygotowanych na podstawie metodyki, testów potwierdzających poprawne funkcjonowanie aplikacji wraz ze wszystkimi funkcjami wymienionymi w ramach Załącznika nr 1A do SIWZ oraz potwierdzającymi prawidłowość działania formularzy, raportów, wydruków i integracji z innymi systemami.
7. Przeszkolenia użytkowników w zakresie w jakim modyfikacji uległ interfejs graficzny użytkownika i/lub przebieg procesów w systemie.
8. Przedstawienie raportu z migracji zawierającego raporty z testów oraz potwierdzenie przeniesienia danych pomiędzy systemami.
9. Uruchomienia i wdrożenia systemu na nowej wydajniejszej bazie danych wraz z asystą uruchomieniową w zakresie w jakim modyfikacji uległ interfejs graficzny użytkownika i/lub przebieg procesów w systemie.

10. Przeszkolenia administratorów Zamawiającego z nowej konfiguracji systemu.
11. Świadczenia usług gwarancyjnych dla prac migracyjnych zgodnie z Umową.
12. Wykonawca ponosi odpowiedzialność za ewentualne szkody, wyrządzone przez jego pracowników, powstałe w wyniku działań prowadzonych przez Wykonawcę na bazach danych posiadanych przez Zamawiającego systemów.
13. Świadczenia usług gwarancyjnych dla wszystkich nowo dostarczanych modułów, licencji związanych z wdrożeniem zgodnie z Umową.

II.3.10 Przenoszenie danych (migracja)

Wykonawca jest odpowiedzialny za przeprowadzenie pełnego procesu migracji danych pomiędzy obecnie użytkowaną bazą SYBASE ASE systemu HIS na nowy wydajniejszy system zarządzania bazą danych.

Zamawiający na etapie realizacji umowy zapewni Wykonawcy dostęp do bazy danych obecnie użytkowanego systemu. Zamawiający do przeprowadzenia migracji bazy danych udostępni interfejs administracyjny serwerów baz danych w trybie odczytu. Wykonawca nie może ingerować w dane ani strukturę danych jak i samych baz danych obecnie użytkowanego systemu HIS CGM CLININET w celu przeprowadzenia procesu migracji danych.

Wykonawca w ramach procesu migracji systemu CGM CLININET do wydajniejszej bazy danych dostarczy, zainstaluje, skonfiguruje oraz dokona strojenia do wydajnej pracy systemu środowisko Systemu HIS aby uzyskać następującą konfigurację systemu.

Szczegółową konfigurację uwzględniającą również powiązanie z istniejącą infrastrukturą Zamawiającego Wykonawca zaprojektuje i przedstawi do akceptacji Zamawiającego w procesie analizy przedwdrożeniowej w projekcie technicznym migracji.

Tabela: struktura baz danych wymagających migracji

L.P.	OPIS	SZCZEGÓŁY
1.	Ilość baz danych	1 instancja Serwera Sybase Adaptive Server Enterprise 5 baz danych: CliniNET_PRD (CliniNET, wersja produkcyjna) CliniNET_TRN (CliniNET, wersja treningowa) CTNControl (NetRAAD) IMAGE (NetRAAD) uhc_contracts (STER)
2.	Rodzaj baz danych	Bazy relacyjne

3.	Struktura poszczególnych baz danych	relacyjna
4.	Rodzaje i ilość tabel	tabele zgodne z bazą danych Sybase – CliniNET_PRD - 4494 tabel CliniNET_TRN - 4494 tabel CTNControl - 10 tabel IMAGE - 117 tabel uhc_contracts - 213 tabel
5.	Zakres danych w tabelach	dane medyczne z lat 2009 - 2020
6.	Opis danych w tabelach	pacjenci, słowniki, dane rozliczeniowe, dane statystyczne, kolejki oczekujących, wszystkie dane ze wszystkich tabel dla części białej i szarej.
7.	Relacje pomiędzy danymi	Struktura bazy danych jest znormalizowana (do trzeciej postaci normalnej 3NF), bez redundancji (powielania danych).
8.	Zainstalowane procedury po stronie serwera bazy danych	Po stronie serwera bazy danych działają procedury odpowiedzialne za: a) Kopię zapasową i przywracanie bazy danych b) Weryfikację / naprawę spójności c) Reorganizację (defragmentację) bazy danych d) Aktualizację statystyk optymalizatora
9.	Logiczne powiązania pomiędzy tabelami w bazie danych	Bd.
10.	Rozmiar baz danych	CliniNET_PRD 394880,0 MB CliniNET_TRN 394880,0 MB CTNControl 374,0 MB IMAGE 35088,0 MB uhc_contracts 12304,0 MB
11.	Sposób migracji	Wbudowane w Sybase ASE narzędzie BCP (eksport / import danych do postaci tekstowej, zbliżonej do CSV)

12.	Informacje na temat spójności danych	dane są spójne

II.3.11 Przebieg procesu migracji

W procesie planowania i realizowania migracji danych wymagane jest planowanie i przeprowadzenie procesu migracji danych przez Wykonawcę przy uwzględnieniu minimum następujących faz/kroków, po przeprowadzonym procesie instalacji systemów i aplliance systemów:

1. **Przygotowanie planu migracji danych** - ustalenie zakresu danych do migracji, sposoby i zakres danych do poprawienia, struktur pośrednich, sposobu przekazania danych, sposobów weryfikacji i innych szczegółów potrzebnych do prawidłowej migracji wszystkich danych wymaganych przez Zamawiającego. Szczegółowy opis wymagań dla planu migracji zawarto w części „Analiza przedwdrożeniowa"
2. **Pobranie danych do struktur pośrednich** – czynność dotyczy przygotowania i wykonania uzgodnionych w planie migracji skryptów pobierających dane do struktur pośrednich (np. testowa baza danych, pliki XML) i eksportu danych do tych struktur. W ramach tego kroku Wykonawca zobowiązany jest do wykonania procesu podniesienia jakości danych słownikowych.
3. **Weryfikacja poprawności danych w strukturach pośrednich** – weryfikacja poprawności procesu exportu danych z systemu źródłowego i importu do struktur pośrednich. W przypadku wystąpienia błędów przy weryfikacji danych w strukturach pośrednich, ustalana jest przyczyna błędu. Jeżeli przyczyna leży w złym pobraniu danych z systemu źródłowego proces wraca do kroku „Pobranie danych do struktur pośrednich". Jeżeli problem dotyczy błędu w procedurach importu danych należy poprawić te procedury i ponownie dokonać importu i weryfikacji danych.
4. **Migracja testowa** - w celu realizacji migracji testowej Wykonawca zobowiązany jest do wykonania kopii docelowego środowiska wydajnej bazy danych na infrastrukturze Zamawiającego i przeprowadzenia kompletnego zasilania danymi tego środowiska za pomocą skryptów i algorytmów, które będą wykorzystywane przy docelowej migracji. Celem migracji testowej jest przetestowanie procedur eksportu/importu danych, procedur czyszczenia, uzupełniania, agregacji danych, procedur weryfikacji danych. Migracja testowa co do zasady powinna być wykonywana na pełnych danych. Dopuszcza się w niektórych szczególnie wymagających obszarach (ze względu na ilość danych) realizację migracji testowej na reprezentatywnej próbce danych, po wcześniejszym ustaleniu i zgodzie Zamawiającego.
5. **Weryfikacja migracji testowej** – w ramach procesu weryfikacji procesu migracji testowej przewiduje się wykorzystanie następujących metod sprawdzania poprawności jej wykonania:

a) **Szczegółowa weryfikacja zapis po zapisie -** jest możliwa tylko jeżeli zbór migrowanych danych nie jest liczny i polega na porównaniu danych w starym rozwiązaniu oraz w nowym Systemie zapis po

zapisie. Dla ułatwienia tego porównania Dostawca Systemu może w niektórych przypadkach przygotować zestawienia tabelaryczne danych z nowego systemu eksportowanie do arkusza kalkulacyjnego lub wydrukowane. Wtedy porównanie polega na zaznaczeniu każdego poprawnego zapisu na wydruku lub w arkuszu.

b) **Porównanie skryptami -** weryfikacja polegająca na uruchomieniu napisanych wcześniej skryptów porównujących dane znajdujące się w nowym Systemie z danymi źródłowymi zapisanymi w tabelach systemu testowego i źródłowego. W takim przypadku raport zgodności / różnic powinien być automatycznie wygenerowany.

c) **Wyrywkowa kontrola danych przez użytkowników -** weryfikacja przeprowadzana przez użytkowników docelowych Systemu, mających dostęp do nowego środowiska testowego Systemu oraz Systemu źródłowego. Polega na wyszukaniu wybranych danych w jednym i drugim systemie oraz ich porównaniu. Wykonawca wykona na środowisku testowym uzgodniony na etapie analizy przedwdrożeniowej zestaw testów funkcjonalnych systemu i przedstawi Zamawiającemu raport z ich realizacji. Dodatkowo Wykonawca udostępni wskazanym pracownikom Zamawiającego środowisko testowe na okres min. 2 tygodni tak by mogli oni sprawdzić poprawność działania systemu po migracji wyżej opisaną metodą.

d) **Porównanie raportów i wydruków z Systemu źródłowego oraz Systemu testowego -** ma polegać na uruchomieniu i porównaniu raportów/wydruków wygenerowanych z Systemu testowego oraz Systemu źródłowego.

e) **Porównanie formularzy dokumentacji medycznej z Systemu źródłowego oraz Systemu testowego -** ma polegać na uruchomieniu i porównaniu formularzy wygenerowanych z Systemu testowego oraz Systemu źródłowego.

f) **Weryfikacja statystyczna –** ma polega na stworzeniu kryteriów poprawności dla migrowanych danych np. liczby rekordów w obydwu systemach dla konkretnych tabel w bazie danych, wartość i liczby świadczeń przekazanych do NFZ itp. Wykonaniu przez dostawcę zestawień porównawczych z obydwu systemów, które umożliwią stwierdzenie poprawności migracji.

W ramach testowania poprawności migracji zostaną zrealizowane minimum następujące testy:

- Testy funkcjonalne
- Testy integracji

Zgodnie z metodyką opracowaną na odrębnym etapie i części zamówienia.

6. **Migracja docelowa produkcyjna** – właściwa migracja, po której rozpoczyna się produkcyjną pracę w nowym Systemie. W przypadku braku stwierdzonych istotnych problemów w trakcie wcześniejszych kroków procesu migracji Zamawiający podejmuje decyzję o przeprowadzeniu procesu migracji do nowego, docelowego Systemu opartego o wydajniejszą bazę danych. Wykonawca po procesie migracji jest zobowiązanych do weryfikacji poprawności

przeniesionych danych – końcowa weryfikacja danych poprzez wykonanie testów poprawności migracji (walidacji danych po migracji) oraz testów wydajności. Pozytywny wynik kończy proces migracji danych.

Wykonawca zobowiązany jest zabezpieczyć trwale dane z systemu źródłowego z momentu migracji danych w postaci kopii bezpieczeństwa danych systemu źródłowego i w przypadku niepowodzenia procesu migracji w założonym harmonogramie przywrócić działanie poprzedniego systemu. Kopie danych oraz systemu w wersji użytkowanej przez Zamawiającego w liczbie sztuk 2 zostaną przekazane Zamawiającemu.

Wykonawca przeprowadzać będzie migracje w siedzibie Zamawiającego. W przypadku, gdy nie będzie to możliwe, Wykonawca zobowiązany będzie do zabezpieczenia pozyskanych od Zamawiającego migrowanych danych w sposób uniemożliwiający wejście w ich posiadanie przez osoby nieupoważnione do ich przetwarzania. Po wykonaniu migracji, wszelkie dane pozyskane w toku migracji przez Wykonawcę zamówienia muszą zostać usunięte ze wszystkich nośników Wykonawcy w sposób uniemożliwiający ich odzyskanie. Jeżeli wystąpi konieczność przekazania Wykonawcy danych do migracji poza siedzibę Zamawiającego, przekazanie będzie się odbywać protokolarnie upoważnionemu przedstawicielowi Wykonawcy, a prace związane z obróbką pozyskanych danych odbywać się będą jedynie w siedzibie Wykonawcy. Wykonawca nie jest upoważniony do przekazywania danych z migracji innym podmiotom.

Dodatkowe wymagania dla procesu migracji zawiera poniższa tabela:

NR WYMAGANIA	OPIS
1	W ramach procesu migracji Wykonawca zobowiązany jest do zachowania ciągłości procedur i procesów realizowanych przez Zamawiającego w szczególności musi zachować ciągłość i format wszystkich numeracji stosowanych w procesach leczenia (nr księgi głównej, ksiąg zabiegowych, nr kartotek pacjentów itp.)
2	W procesie migracji zostaną przeniesione wszystkie dane historyczne zgromadzone i przetwarzane obecnie przez Zamawiającego w systemie HIS CGM CLININET
3	Proces migracji musi zapewnić ciągłość rozliczeń z NFZ zarówno w zakresie nowych danych wprowadzanych do zmigrowanego Systemu jak i korekty danych wcześniej przekazanych do płatników (NFZ i inni).
4	Wykonawca wykona migrację danych do nowej wydajniejszej bazy danych zgodnie z zaakceptowanym planem migracji danych. Wykonawca jest odpowiedzialny za wykonanie migracji wszystkich danych potrzebnych do prawidłowego działania Systemu.
5	Proces migracji nie może zaburzyć wzajemnych powiązań logicznych danych.

	Wzajemne relacje pomiędzy danymi w systemie muszą być zachowane (integralność danych).
6	Migracja musi być przeprowadzona w dwóch etapach: • migracja testowa • migracja produkcyjna.
7	Warunkiem możliwości wykonania migracji produkcyjnej jest akceptacja przez Zamawiającego wyników migracji testowej na podstawie raportu z testów migracji przedstawionego przez Wykonawcę.
8	Wykonawca ponosi odpowiedzialność za poprawność danych migrowanych do nowego Systemu i jest zobowiązany bez zbędnej zwłoki usunąć wszelkie skutki wynikające z błędów migracji i dokonać naprawy danych i działania Systemu nawet w przypadku, jeżeli nieprawidłowości wystąpią w procesie eksploatacji systemu po odbiorze procedury migracji. Zobowiązanie to dotyczy całości trwania okresu umowy oraz okresu gwarancji/rękojmi.

II.3.12 Asysta techniczna w procesie migracji produkcyjnej

W ramach procesu migracji produkcyjnej Wykonawca przez okres 10 dni od jej wykonania zobowiązany jest prowadzić asystę techniczną u Zamawiającego. W ramach tej asysty zobowiązany jest zapewnić obecność u Zamawiającego począwszy od 1 dnia roboczego (co najmniej 8h) po wykonaniu startu produkcyjnego systemu na nowej bazie danych następujących specjalistów:

1. Administrator bazy danych - 1 osoba 2 dni po starcie produkcyjnym
2. Wdrożeniowiec systemu HIS – 2 osoby 5 dni po starcie produkcyjnym
3. Programista – projektant formularzy – 1 osoba 5 dni po starcie produkcyjnym

Osoby te zobowiązane są na bieżąco wspierać pracowników Zamawiającego w identyfikacji i usuwaniu usterek, które mogą powstać po procesie migracji. Zamawiający zastrzega sobie prawo skrócenia tego okresu, jeżeli uzna, że stabilność systemu po migracji jest wystarczająca.

II.3.13 Testy migracji

Wykonawca ma obowiązek wykonać testy całości projektu, ale również, odrębnie testy samej migracji bazy danych razem z walidacją tych danych. Testy zostaną przeprowadzone w sposób opisany poniżej, a metodologia prowadzenia testów ma zostać oparta o metodologię testów całości wdrożenia projektu.

W ramach realizacji przedmiotu umowy Wykonawca zobowiązany jest przeprowadzić zestaw testów potwierdzających poprawność wykonania migracji. W skład testów realizowanych w ramach procesu migracji systemu HIS powinny zostać zrealizowane minimum następujące testy:

1. Testy funkcjonalne – zestaw testów potwierdzających możliwość realizacji kluczowych procesów na środowisku systemu po migracji na nowy silnik bazy danych.
2. Testy wydajnościowe – testy mające na celu potwierdzenie, że założone w procesie migracji wskaźniki zwiększenia wydajności systemu poprzez migrację na nowy, wydajniejszy silnik bazy danych zostały osiągnięte.
3. Testy integracji – testy potwierdzające zdolność systemu po migracji do współpracy z innymi systemami Zamawiającego.
4. Testy integralności i poprawności zmigrowanych danych w nowym, wydajniejszym SZBD
5. Testy bezpieczeństwa - testy obejmować będą swym zakresem:
   a. Testy penetracyjne wskazanych zasobów wykonywane metodą white, black lub grey -box
   b. Testy bezpieczeństwa aplikacji wytworzonych i dostarczonych w ramach projektu wskazanych przez Zamawiającego na etapie Analizy przedwdrożeniowej
   c. Testy poprawności konfiguracji i parametryzacji sprzętu serwerowego oraz sprzętu sieciowego aktywnego na styku komunikacji z zewnętrzną siecią.

Testy te będą prowadzone w środowisku produkcyjnym systemu teleinformatycznego w co najmniej 2 iteracjach.

W przypadku zidentyfikowania Błędów lub Wad Wykonawca jest zobowiązany do ich poprawy przed odbiorem Przedmiotu Zamówienia.

II.3.14 Dokumentacja z przeprowadzonych testów migracji

Dokumentacja będąca podstawą przeprowadzenia testów zostanie opracowana przez Wykonawcę na etapie analizy przedwdrożeniowej. Dokumentacja testowa będzie obejmowała następujące rodzaje dokumentów:

1. Plan testów
2. Scenariusz testowe
3. Przypadki testowe
4. Dane do testów.

Plan i scenariusze będą zgodne z powszechnie stosowanymi zasadami i praktykami.

Plan testów określać będzie w szczególności:

1. ogólne zasady przeprowadzania testów,
2. opis środowiska testowego;
3. kolejność wykonywania scenariuszy testowych;
4. klasyfikację wykrytych problemów testowych;
5. kryteria sukcesu dla poszczególnych kategorii testów.

Scenariusze będą zapewniać pokrycie wszystkich procesów systemu HIS kluczowych dla działalności Zamawiającego określonych na etapie analizy przedwdrożeniowej. Każdy scenariusz określać będzie:

- dane, które muszą być wprowadzone do systemu przed uruchomieniem scenariusza;
- kolejność czynności, wykonywanych w czasie testu oraz dane, wprowadzane do systemu w czasie testu;
- oczekiwaną reakcję systemu na wykonane czynności i wprowadzone dane.

Przypadki testowe i dane testowe, w tym wszelkie materiały eksploatacyjne dostarczone będą przez Wykonawcę. Zamawiający zobowiązany jest do współpracy z Wykonawcą przy przygotowywaniu scenariuszy testowych i danych testowych, przeprowadzaniu testów oraz przygotowaniu wyników testów. Zamawiający zastrzega sobie prawo zmiany scenariusza testu akceptacyjnego.

Zamawiający dopuszcza przeprowadzenie testów automatycznych, o ile w planie testów zostanie wyspecyfikowany zakres tych testów i uzyska on akceptację Zamawiającego.

Testy będą przeprowadzone w terminie przewidzianym w harmonogramie, zgodnie z zaakceptowanym planem testów.

Testy zostaną wykonane z użyciem środowiska testowego migracji chyba, że plan testów będzie przewidywał inaczej, na bazie reprezentatywnej próbki danych eksploatacyjnych. Zakres testów nie może wykraczać poza merytoryczny zakres projektu. Test może zostać przerwany, jeżeli z jakiejkolwiek przyczyny nie może być kontynuowany (np. poważny błąd w oprogramowaniu lub awaria systemu). Test taki powinien zostać powtórzony lub kontynuowany w innym terminie po obustronnym uzgodnieniu.

Po zakończeniu testowania każdego z obszarów, wyznaczona ze strony Zamawiającego osoba odpowiedzialna za przebieg testowania podpisuje i przekazuje Kierownikowi Projektu ze strony Wykonawcy protokół z testów.

W ramach procesu testowania określa się następujące kategorię błędów:

POZIOM ISTOTNOŚCI	**OPIS**
A/Krytyczny	Zatrzymanie działania Produktu lub błąd uniemożliwiający realizację kluczowego procesu w tym takie obniżenie wydajności, które w praktyce uniemożliwia jego realizację i nie jest możliwe wskazanie obejścia błędu.

B /Wysoki	Zatrzymanie działania Produktu lub realizację kluczowego procesu w tym takie obniżenie wydajności, które w praktyce uniemożliwia jego realizację, ale jest możliwe wskazanie obejścia błędu. Obejście umożliwia weryfikację funkcjonalności występujących „za" błędem.
C /Średni	Zakłócenie pracy Produktu wpływające na weryfikację poprawności przebiegu kluczowego procesu.
D/Niski	Zakłócenie pracy Produktu niewpływające na poprawności przebiegu kluczowego procesu, w tym błędy kosmetyczne interfejsu.

II.3.15 Kryteria Akceptacji Testów

Kryteria akceptacji dla scenariuszy i przypadków testowych

Wynik testu dla Scenariusza Testowego uznaje się za pozytywny, gdy wyniki testów dla wszystkich Przypadków Testowych zawartych w Scenariuszu Testowym są pozytywne. Wynik testu dla Scenariusza Testowego uznaje się za negatywny, gdy wynik testu dla któregokolwiek Przypadku Testowego zawartego w Scenariuszu testowym jest negatywny.

Wynik testu dla Przypadku Testowego uznaje się za pozytywny, gdy opis oczekiwanego rezultatu zamieszczony w polu „Oczekiwany wynik" jest 'zgodny' z faktycznie uzyskanym wynikiem po zakończeniu Przypadku Testowego.

Wynik testu dla Przypadku Testowego uznaje się za negatywny, gdy opis oczekiwanego rezultatu zamieszczony w polu „Oczekiwany wynik" jest 'nie zgodny' z faktycznie uzyskanym wynikiem po zakończeniu Przypadku Testowego. W przypadku, gdy występująca niezgodność jest wynikiem błędnie opisanego Przypadku Testowego, wówczas wynik testu może być uznany za prawidłowy, a błędny opis Przypadku Testowego musi zostać poprawiony przez Wykonawcę. Sytuacja taka musi znaleźć odzwierciedlenie w raporcie z Testów Akceptacyjnych.

Kryteria zakończenia testów sukcesem

Testy są wykonane na podstawie Scenariuszy Testowych zaakceptowanych przez Zamawiającego.

Testy uznaje się za zakończone z sukcesem, gdy:

- przeprowadzono testy z wykorzystaniem 100% zaplanowanych Scenariuszy Testowych,

- brak niezakończonych Scenariuszy Testowych z powodu wystąpienia Incydentu/ów z klasą istotności: B/Wysoki, C/Średni i D/Niski, których liczba wykracza poza dopuszczalny limit określony w tabeli poniżej
- na moment zakończenia Testów Akceptacyjnych brak jest Incydentów z klasą istotności A/Krytyczny.

W przypadku wystąpienia Incydentu, który uniemożliwia wykonanie wszystkich zaplanowanych przypadków Testowych i/lub Scenariuszy Testowych, a który nie wynika z winy Wykonawcy, wówczas zakres testów może zostać zmieniony (wyłączenie przypadków i/lub scenariuszy) na podstawie decyzji podjętej przez Zamawiającego.

W przypadku Scenariuszy Testowych zakończonych negatywnie, w których wystąpiły Incydenty o klasie istotności: B/Wysoki, C/Średni lub D/Niski, wynik ich zakończenia może zostać uznany za pozytywny na podstawie decyzji podjętej przez Kierownika Projektu ze strony Zamawiającego.

Testy uznaje się za zakończone z wynikiem negatywnym, gdy po ich zrealizowaniu otrzymano następujące wyniki:

- istnieje przynajmniej jeden niezakończony Scenariusz Testowy z powodu wystąpienia Incydentu/ów z klasą istotności A/Krytyczny,
- istnieją niezakończone Scenariusze Testowe z powodu wystąpienia Incydentu/ów z klasą istotności: B/Wysoki i C/Średni, których liczba wykracza poza dopuszczalny limit określony w tabeli poniżej, w takim przypadku Scenariusze te nie mogą zostać uznane za zakończone pozytywnie.

W przypadku zakończenia Testów z wynikiem negatywnym, zostanie ustalony plan powtórzenia testów. Wybór scenariuszy do II tury testów zostanie przeprowadzony według następujących zasad:

- Scenariusze Testowe, które otrzymały wynik negatywny z powodu wystąpienie Incydentu/ów.
- Scenariusze Testowe dla funkcjonalności powiązanych z funkcjonalnością Scenariusza Testowego, w którym wystąpiły Incydenty.

Zamawiający zastrzega sobie prawo przeprowadzenia jednej iteracji testów regresji dla scenariuszy z wynikiem pozytywnym.

Kryteria akceptacji testów funkcjonalnych

Dopuszczalna liczba otwartych Incydentów na zakończenie Testów Funkcjonalnych migracji

KATEGORIA BŁĘDU	DOPUSZCZALNA LICZBA PRZYPADKÓW TESTOWYCH Z BŁĘDEM
A/Krytyczny	0
B/Wysoki	2

C/Średni	5
D/Niski	10

Po migracji średni czas reakcji systemu musi być krótszy niż 0,7 sekundy - mierzony według metodyki ustalonej z Zamawiającym na etapie analizy przedwdrożeniowej.

Generowane z nowej wersji systemu pliki wymiany (pliki XML, dokumenty HL7, widoki na bazie danych) posiadają identyczną strukturę i zawartość dla takiego samego zakresu danych jak w dotychczas używanym systemie HIS, co zostanie również uwzględnione opisie raportu z testów.

II.3.16 Specyficzna procedura odbioru części związanej z migracją danych

W ramach części związanej z migracją baz danych dostarczany produkt typu System (system po migracji).

Odbiór produktu typu migracja systemu

Proces odbioru produktu migracja systemu będzie przebiegał następująco:

1. Wykonawca po przeprowadzaniu procesu migracji testowej systemu na wydajniejszą bazę danych przedstawia raport z migracji wg szablonu uzgodnionego na etapie analizy przedwdrożeniowej oraz zgłasza gotowość systemu do testów funkcjonalnych. Raport z migracji musi dokumentować poprawność przeprowadzenia procesu migracji testowej w szczególności kompletność przeniesionych danych.
2. Testy funkcjonalne wykonywane są na podstawie dokumentacji testowej zatwierdzonej na etapie analizy przedwdrożeniowej z zastrzeżeniem, że dokumentacja ta będzie uwzględniała pełny przebieg kluczowych dla Zamawiającego procesów biznesowych. Jako pełny przebieg rozumie się testowanie zarówno ścieżek pozytywnych jak i negatywnych dla procesów.
3. Testy funkcjonalne wykonywane są na dokumentacji testowej opracowanej w ramach analizy przedwdrożeniowej.
4. Za realizację testów odpowiada Wykonawca przy współudziale Zamawiającego. Zamawiający zastrzega sobie prawo samodzielnej realizacji testów przy lub bez obecności Wykonawcy. W przypadku realizacji testów bez obecności wykonawcy, Zamawiający zobowiązuje się do opisu wykrytych błędów w sposób umożliwiający odtworzenie błędu Wykonawcy (opis powtarzalnej ścieżki dojścia do błędu wraz z zestawem danych testowych). Informacje takie będę przekazane w dokumencie będącym protokołem z sesji odbytych testów systemu przez Zamawiającego.
5. Jeżeli w procesie testowania uwidocznione zostały błędy uniemożliwiające odbiór systemu w ramach raportu z testów są one uwidaczniane w tym raporcie wraz z ustaleniem terminu

przeprowadzanie II tury testów. Kryteria odbiorowe dla poszczególnych rodzajów testów określone są w pkt. „Testy".

6. Wykonawca w uzgodnionym terminie przedstawia system do II tury testów. W ramach II tury testów weryfikowane są scenariusze, dla których stwierdzono występowanie błędów w ramach I tury. Zamawiający zastrzega sobie prawo wykonania testów regresji dla scenariuszy testowych które przebiegły poprawnie w II turze.
7. Każda tura testów kończy się raportem z testów.
8. W przypadku spełniania warunków odbioru testów funkcjonalnych migracji systemu Zamawiający i Wykonawca podpisują protokół odbioru testów funkcjonalnych migracji.
9. W przypadku pozytywnej weryfikacji raportu z migracji i testów funkcjonalnych migracji Zamawiający podejmuje decyzję o realizacji migracji produkcyjnej.
10. Po przeprowadzaniu uruchomienia produkcyjnego systemu po migracji w terminie nie wcześniej niż 5 dni po, Wykonawca przedstawi raport z migracji produkcyjnej systemu wg szablonu uzgodnionego na etapie analizy przedwdrożeniowej. Raport będzie zawierał raporty z wydajności systemu sprzed i po migracji systemu. Raporty te powinny umożliwiać porównanie:
    a. Czasu zapisu do bazy danych systemu dla tych samych lub porównywalnych danych.
    b. Czasu odpowiedzi bazy danych na zapytania systemu dla tych samych lub porównywalnych zapytań.
    c. Czasu wykonania raportów, które w systemie przed migracją trwały bardzo długo np. raportów sumarycznych o liczbie wykonanych procedur medycznych w długim okresie czasu.
11. Na podstawie raportu z migracji produkcyjnej systemu Zamawiający dokona odbioru migracji systemu poprzez podpisanie protokołu odbioru.
12. Zamawiający zastrzega sobie prawo odmowy podpisania protokołu odbioru, jeżeli w dniu odbioru będzie występował błąd blokujący lub 5 awarii systemu zgłoszonych przez Zamawiającego po dacie startu produkcyjnego systemu po migracji w okresie 2 tygodni. Przy czym wystąpienie błędu związane będzie z procesem migracji i błąd nie będzie odtwarzalny na obecnej (przed migracją) u zamawiającego instalacji systemu HIS.
13. Odbiór migracji systemu zostanie potwierdzony protokołem odbioru podpisanym przez obie strony.

Zamawiający zastrzega sobie prawo odbioru warunkowego migracji systemu, w którym stwierdzono wady, ale nie są one na tyle istotne by wstrzymywać przebieg prac projektowych. W takim przypadku w protokole odbioru migracji zawierane są klauzule wskazujące listę wad do usunięcia wraz ze wskazaniem terminu dostarczenia produktu bez wad.

II.3.17 Migracja danych – w przypadku wymiany systemu na nowy

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

Systemy podlegające ewentualnej migracji: CGM Clininet (część medyczna).

Informacje o bazie danych HIS zawarte są w pkt. II.3.10 SOPZ - Przenoszenie danych (migracja).

Zamawiający zapewnieni dane do migracji w postaci plików CSV lub XLS zawierających dane do migracji wraz z dokumentacją umożliwiającą pełną identyfikację zawartości tych plików.

Informacje techniczne umożliwiające migrację:

L.P.	OPIS	SZCZEGÓŁY
1.	**Ilość baz danych**	**7 szt.:** **- CliniNET_PRD (CliniNET, wersja produkcyjna),** **- CliniNET_TRN (CliniNET, wersja treningowa),** **- CTNControl (NetRAAD),** **- IMAGE (NetRAAD),** **- uhc_contracts (STER),** **- system obsługi Apteki,** **- system obsługi Laboratorium.**
2.	**Rodzaj baz danych**	**Bazy relacyjne, złożone**
3.	**Struktura poszczególnych baz danych**	**relacyjna**
4.	**Rodzaje i ilość tabel**	**Tabele zgodne z bazą danych Sybase –** **CliniNET_PRD - 4494 tabel** **CliniNET_TRN - 4494 tabel** **CTNControl - 10 tabel** **IMAGE - 117 tabel** **uhc_contracts - 213 tabel** **system obsługi Apteki,** **system obsługi Laboratorium**
5.	**Rozmiar baz danych**	**CliniNET_PRD 394880,0 MB** **CliniNET_TRN 394880,0 MB** **CTNControl 374,0 MB** **IMAGE 35088,0 MB** **uhc_contracts 12304,0 MB**
6.	**Zakres danych w tabelach**	**dane medyczne z lat 2009 - 2021**

7.	**Opis danych w tabelach**	**W załączniku 1B w postaci raportu HTML**
8.	**Informacje na temat spójności danych**	**dane są spójne**

W przypadku migracji danych rozliczeniowych, Zamawiający zapewni dostęp do wszystkich sprawozdawanych danych w ramach komunikatów ŚWIAD. Wszystkie dane zawarte są w bazie uhc_contracts (STER).
Wykonawca przy wsparciu ze strony Zamawiającego, będzie miał możliwość wykonania eksportu struktury i danych zawartych w bazach w celu wdrożenia nowego systemu.

II.3.18 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 komórki właściwej ds. 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.

II.3.19 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 Zamawiającego. 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.
1. Wykonawca nie ponosi odpowiedzialności za brak uczestnictwa użytkowników w instruktażach stanowiskowych.
2. 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,
6. Za skuteczne przeprowadzenie instruktażu stanowiskowego uważa się dostępność w ustalonym miejscu i terminie przedstawicieli Wykonawcy, gotowych przeprowadzić instruktaż zgodnie z ustalonym harmonogramem.
7. Wykonawca w ramach instruktażu stanowiskowego przekaże instrukcje do wdrożonego Systemu oraz materiały szkoleniowe. Instruktaże stanowiskowe będą prowadzone w języku polskim
8. 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.
9. 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.
10. Instruktaże stanowiskowe będą prowadzone w dwóch kategoriach:
    a) dla użytkowników oprogramowania SSI – **160 godzin**
    b) dla administratorów – 40 **godzin**
11. Szacowana liczba pracowników Zamawiającego planowanych do instruktaży stanowiskowych **maksimum** 80 osób personelu Zamawiającego i **maksimum** 4 administratorów, w tym:
    a) pracownicy rejestracji: **maksimum** 5 osób
    b) lekarze: **maksimum** 25 osób
    c) pielęgniarki: 50 osób
12. 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.

13. 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.
14. 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.
15. 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:

    a) dostęp do czatu z możliwością zadawania pytań oraz udzielania odpowiedzi,
    b) 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.

Rozdział III. Gwarancja

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

1) **Dostawa i wdrożenie Infrastruktury serwerowej wraz z oprogramowaniem systemowym i narzędziowym i Szpitalnym Systemem Informatycznym:**

a) Infrastruktura serwerowa wraz z oprogramowaniem systemowym i narzędziowym:

Poz. SOPZ	Opis	Okres gwarancji (minimalny)
II.1.1	Serwer wirtualizacyjny	**36 miesięcy***
II.1.2	Serwer do kopii (backup) *,**	**36 miesięcy*, ****
II.1.3	Serwer bazodanowy	**36 miesięcy***
II.1.4	Macierz główna*,**	**36 miesięcy*, ****
II.1.5	Biblioteka LTO	**36 miesięcy***
II.1.6	Przełącznik zasobowy do macierzy	**36 miesięcy*, *** gwarancja producenta**
II.1.7	Zasilacz awaryjny UPS	**24 miesiące***
II.1.8	Szafa Rack	**24 miesiące**
II.3.5	Wyświetlacz gabinetowy 21”	**36 miesięcy**
II.3.5	Wyświetlacz rejestracja 21”	**36 miesięcy**
II.3.5	Wyświetlacz zbiorczy 50’’	**36 miesięcy**
II.3.5	Infokiosk	**24 miesiące***
Il.3.5	Drukarka biletów	**24 miesiące**
II.1.9	Przełącznik LAN	**60 miesięcy**
II.1.10	Przełącznik zarządzający	**60 miesięcy *****
II.1.11	Punkt dostępowy wewnętrzny	**36 miesięcy**
II.1.12	UTM	**60 miesięcy**

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

** W przypadku awarii dysków pozostają one własnością Zamawiającego.

*** Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego.

b) dostawa i wdrożenie Szpitalnego Systemu Informatycznego:

Poz. SOPZ	Opis	Okres gwarancji i usługi gwarancyjnej (minimalny)
II.3.5	System HIS – część medyczna	**60 miesięcy**

	Elektroniczna Dokumentacja Medyczna	
	e-Usługi – część medyczna	

III.1.1 Zakres usług gwarancyjnych dostarczonego oprogramowania aplikacyjnego.

Nazwa Usługi	Przedmiot Usługi
Usługi gwarancyjne	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 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 przez producenta systemu w ramach nadzoru autorskiego w trybie pilnym do ww. oprogramowania aplikacyjnego zmian i poprawek usuwających stwierdzone błędy krytyczne i luki we wbudowanych

	mechanizmach i funkcjach zabezpieczeń, – gotowość przez producenta systemu do odpłatnego wykonania na zlecenie Zamawiającego zaproponowanych przez niego modyfikacji ww. oprogramowania aplikacyjnego.
Konsultacje	Gotowość do świadczenia Zamawiającemu usługi pomocy technicznej i eksploatacyjnej w odniesieniu do ww. oprogramowania aplikacyjnego.

III.1.2 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:

1) **Awaria -** Kategoria Wady w Oprogramowaniu 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

2) **Błąd** - Należy przez to rozumieć Wadę Oprogramowania oznaczającą jego funkcjonowanie niezgodne z opisem w Dokumentacji oraz SOPZ, powodujące błędne zapisy w bazie danych lub uniemożliwiające działanie mniej istotnej funkcjonalności w Systemie.

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

2. Przyjęcie zgłoszenia Wady przez Wykonawcę, odbywać się będzie poprzez dostępny on-line System Zgłaszania i przyjmowania uwag oraz Wad (dalej zwany SZ) przy czym:
   1) System Zgłoszeń dostarczy Wykonawca (będzie on utrzymywany i administrowany przez Wykonawcę), wpis zgłoszenia do SZ będzie dokonywał Zamawiający,
   2) za skuteczne przyjęcie zgłoszenia Wady uważa się będzie wprowadzenie przez Zamawiającego wpisu do SZ zawierającego opis zgłaszanej Wady i termin jej zgłoszenia; w razie trudności z dostępem on-line do SZ, zgłoszenia Wady mogą odbywać się także telefonicznie pod ustalonym numerem telefonu lub pisemnie na formularzu przesyłanym na ustalony adres e-mail, opcjonalnie faksem, których numery i adresy zostaną podane przez Wykonawcę w terminie 15 dni roboczych od dnia podpisania Umowy wraz ze wzorem formularza zgłoszenia Wady.

3. W przypadku, w którym wykonanie Umowy związane będzie z modernizacją lub rozbudową istniejącego oprogramowania, gwarancja obejmuje całość oprogramowania modernizowanego lub rozbudowywanego.
4. Gwarancja musi zapewniać wymianę uszkodzonego sprzętu, kabli i elementów oraz zapewniać dostęp do aktualizacji oprogramowania, bez wiedzy i wsparcia technicznego producenta.
5. W ramach gwarancji Wykonawca będzie świadczył następujące usługi:
   1) 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 wirtualizacyjny
- Serwer do kopii (backup)
- Serwer bazodanowy
- Biblioteka LTO
- Przełącznik zasobowy do macierzy
- Zasilacz awaryjny UPS
- Przełącznik LAN
- Przełącznik Zarządzający
- UTM

KWALIFIKACJA ZGŁOSZENIA WADY	OKRES DOSTĘPNOŚCI WYKONAWCY	ROZWIĄZANIE ZASTĘPCZE*	CZAS REAKCJI WYKONAWCY	CZAS NAPRAWY
AWARIA	W dni robocze pomiędzy 8.00 a 16.00. Zgłoszenie przesłane po 16.00, traktowane jest jak zgłoszenie przyjęte w następnym dniu roboczym o 8.00. Zgłoszenie przyjęte w dniu ustawowo lub	nie dotyczy	1 dzień roboczy od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 10 dni od czasu przyjęcia zgłoszenia
USTERKA		nie dotyczy	1 dzień roboczy od czasu przyjęcia zgłoszenia	niezwłocznie nie później niż 14 dni od dnia przyjęcia zgłoszenia

KWALIFIKACJA ZGŁOSZENIA WADY	OKRES DOSTĘPNOŚCI WYKONAWCY	ROZWIĄZANIE ZASTĘPCZE*	CZAS REAKCJI WYKONAWCY	CZAS NAPRAWY
	dodatkowo wolnym od pracy - traktowane jest jak przyjęty o godz. 8.00 najbliższego dnia roboczego			

***nie dotyczy wymiany sprzętu**

Wymagane jest zapewnienie technicznego dla przełącznika LAN oraz przełącznika Zarządzającego (niezależnego od zgłaszania usterek) wsparcia telefonicznego w trybie 8x5 przez okres 8 lat. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.

Tabela 2. Usługi gwarancji dla Infrastruktury serwerowej:

- 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 4 godziny od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 2 dni od czasu przyjęcia zgłoszenia
USTERKA		nie dotyczy	niezwłocznie nie później niż 5 dni roboczych od dnia przyjęcia zgłoszenia	niezwłocznie nie później niż 14 dni od dnia przyjęcia zgłoszenia

Tabela 3. Usługi gwarancji dla Infrastruktury serwerowej:

- Szara rack
- Wyświetlacz gabinetowy 21”
- Wyświetlacz rejestracja 21”

- Wyświetlacz zbiorczy 50”
- Infokiosk
- Drukarka biletów
- Punkt dostępowy wewnętrzny

KWALIFIKACJA ZGŁOSZENIA WADY	OKRES DOSTĘPNOŚCI WYKONAWCY	ROZWIĄZANIE ZASTĘPCZE	CZAS REAKCJI WYKONAWCY	CZAS NAPRAWY
AWARIA	24/5/365	nie dotyczy	niezwłocznie, nie później niż 44 godzin od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 14 dni od czasu przyjęcia zgłoszenia
USTERKA		nie dotyczy	niezwłocznie nie później niż 5 dni roboczych od dnia przyjęcia zgłoszenia	niezwłocznie nie później niż 30 dni od dnia przyjęcia zgłoszenia

Tabela 4. Usługi gwarancyjne dla Szpitalnego Systemu Informatycznego

KWALIFIKACJA ZGŁOSZENIA WADY	OKRES DOSTĘPNOŚCI WYKONAWCY	ROZWIĄZANIE ZASTĘPCZE/ TYMCZASOWE	CZAS REAKCJI WYKONAWCY	CZAS NAPRAWY
AWARIA	W dni robocze pomiędzy 8.00 a 16.00. Zgłoszenie przesłane po 16.00, traktowane jest jak zgłoszenie przyjęte w następnym dniu roboczym o 8.00. Zgłoszenie przyjęte w dniu ustawowo lub dodatkowo wolnym od pracy - traktowane jest jak	może wprowadzić rozwiązanie tymczasowe, doraźne rozwiązujące problem awarii; w tym przypadku dalsza obsługa usunięcia dotychczasowej awarii będzie traktowana jako błąd	1 dzień roboczy od czasu przyjęcia zgłoszenia	3 dni robocze od czasu rozpoczęcia czynności gwarancyjnych

KWALIFIKACJA ZGŁOSZENIA WADY	OKRES DOSTĘPNOŚCI WYKONAWCY	ROZWIĄZANIE ZASTĘPCZE/ TYMCZASOWE	CZAS REAKCJI WYKONAWCY	CZAS NAPRAWY
BŁĄD	przyjęty o godz. 8.00 najbliższego dnia roboczego	nie dotyczy	do 15 dni roboczych od dnia przyjęcia zgłoszenia	Do 30 dni roboczych od czasu rozpoczęcia czynności serwisowych
USTERKA		nie dotyczy	niezwłocznie nie później niż 30 dni roboczych od dnia przyjęcia zgłoszenia	niezwłocznie nie później niż 30 dni roboczych od dnia przyjęcia zgłoszenia

2) dopuszcza się zmianę kwalifikacji zgłoszenia Wady, po uprzedniej zgodzie Zamawiającego udokumentowanej na panelu zgłoszeń lub w korespondencji email. Do czasu potwierdzenia zmiany kwalifikacji, uznaje się za obowiązującą kwalifikację pierwotną,
3) czasy naprawy mogą być inne niż wskazane w powyższych tabelach, jeżeli Zamawiający zaakceptuje zmianę kwalifikacji zgłoszenia, o której mowa w punkcie 2),
4) w przypadku braku możliwości usunięcia Wady lub przedstawienia rozwiązania zastępczego zdalnie, Wykonawca zobowiązany jest do świadczenia gwarancji bezpośrednio w lokalizacji Zamawiającego,
5) usunięcie Wady Oprogramowania, nastąpi poprzez przekazanie poprawki lub nowej wersji. Każda nowa poprawka lub nowa wersja musi posiadać unikalny numer.
6) 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,
7) wykonywania usług gwarancyjnych dla Oprogramowania na poniższych zasadach:

a) wykonywania modyfikacji bez wezwania lub na pisemne zgłoszenie Zamawiającego w celu dostosowania wszystkich elementów Oprogramowania do obowiązujących przepisów prawnych,

b) przekazania Zamawiającemu informacji o nowych wersjach Oprogramowania drogą elektroniczną na wskazany adres e-mail Zamawiającego lub poprzez dedykowany panel zgłoszeń,

c) W uzasadnionych przypadkach, Zamawiający dopuści, aby Wykonawca udostępnił odpowiednie zmiany w terminach umożliwiających Zamawiającemu wywiązanie się ze zmienionych przepisów prawa.

d) każda nowa wersja musi posiadać unikalny numer;

e) wraz z nową wersją Wykonawca zobowiązany jest do przekazania nowej wersji Dokumentacji Powykonawczej wraz z procedurą instalacji oraz informacją o parametryzacji i konfiguracji.

f) 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.

III.1.3 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 na urządzenia musi być świadczona przez firmę autoryzowaną przez producenta lub jego przedstawicielstwo w Polsce w przypadku, gdy Oferent nie posiada takiej autoryzacji.
4. Zamawiający ustala procedurę zdalnego dostępu Wykonawcy do Oprogramowania:
   1) Wykonawca drogą elektroniczną poprzez e-mail, prześle Zamawiającemu wniosek o uzyskanie zdalnego dostępu do Oprogramowania, wskazując co najmniej:
      a) imię i nazwisko pracownika Wykonawcy, któremu zostanie przyznany dostęp,

b) nazwa i adres IP zasobu (bazy danych/oprogramowania), który zostanie udostępniony,
c) usługi sieciowe, które zostaną udostępnione,
d) okres czasu, na który będzie aktywowany dostęp,
e) numer zgłoszenia gwarancyjnego,
f) przyczyna złożenia wniosku,
g) opis czynności, które zostaną wykonane,
h) imię i nazwisko pracownika Wykonawcy uprawnionego do złożenia wniosku.

2) osoba wyznaczona przez Zamawiającego zaopiniuje wniosek i w formie elektronicznej poprzez e-mail odpowie, podając informację o zgodzie lub jej braku.
3) po zakończeniu prac Wykonawca ma obowiązek przesłać Zamawiającemu raport z wykonanych prac z wykorzystaniem zdalnego dostępu, podając czas ich trwania i zakres.
4) każdy zdalny dostęp do Oprogramowania musi być przez Wykonawcę odnotowany w Systemie Zgłoszeń,
5) dostęp do zasobów Zamawiającego musi być zgodny z obowiązującą u niego polityką bezpieczeństwa. Zamawiający udostępni procedury bezpieczeństwa Wykonawcy, którego oferta zostanie wybrana jako najkorzystniejsza, po podpisaniu umowy.
6) W przypadku dostarczenia nowej lub zmodyfikowanej wersji Oprogramowania wymagającego aktualizacji lub wymiany Oprogramowania dostarczonego w ramach niniejszej Umowy, Wykonawca w ramach gwarancji ma obowiązek wymiany lub aktualizacji także tego Oprogramowania.

5. W ramach usług gwarancyjnych dla Oprogramowania SSI Wykonawca zobowiązuje się do:

a) wykonywania modyfikacji bez wezwania lub na pisemne zgłoszenie Zamawiającego w celu dostosowania wszystkich elementów Oprogramowania SSI do obowiązujących przepisów prawnych,
b) przekazania Zamawiającemu informacji o nowych wersjach oprogramowania drogą elektroniczną na wskazany adres e-mail Zamawiającego lub poprzez dedykowany panel zgłoszeń,
a) 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;
b) 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;

c) wraz z nową wersją oprogramowania Wykonawca zobowiązany jest do przekazania nowej wersji Dokumentacji uwzględniającej dokonane zmiany wraz z procedurą instalacji oprogramowania oraz informacją o parametryzacji i konfiguracji.

d) 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 8.00 do 16.00 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.