

Znak sprawy: ZP/12/2020

Załącznik nr 3 do SIWZ

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

W POSTĘPOWANIU NA:

Dostawa i wdrożenie eUsług i oprogramowania dla Szpitalnego Systemu Informatycznego wraz z usługą migracji danych do nowego środowiska bazodanowego oraz dostawą niezbędnej infrastruktury technicznej.

**DLA
SAMODZIELNEGO PUBLICZNEGO KLINICZNEGO SZPITALA OKULISTYCZNEGO
W WARSZAWIE**

*w Projekcie „Wprowadzenie nowoczesnych e-usług w podmiotach
lecniczych nadzorowanych przez Ministra Zdrowia”*

Warszawa 2020

ROZDZIAŁ I. ZAŁOŻENIA POCZĄTKOWE ORAZ WYMAGANIA OGÓLNE.....	3
I.1	WPROWADZENIE.....3
I.2	CEL PROJEKTU3
I.3	INTEGRACJA Z CENTRALNYM SYSTEMEM E-ZDROWIE4
I.4	AKTY PRAWNE.....5
I.5	OGÓLNY OPIS PRZEDMIOTU ZAMÓWIENIA6
I.6	TERMIN REALIZACJI PRZEDMIOTU ZAMÓWIENIA.....8
I.7	ORGANIZACJA WDROŻENIA9
I.7.1	<i>Założenia podstawowe</i>9
I.7.2	<i>Przygotowanie Dokumentacji</i>11
I.7.3	<i>Harmonogram wdrożenia</i>11
I.7.4	<i>Analiza Przedwdrożeńiowa</i>12
I.7.5	<i>Dokumentacja Powykonawcza</i>13
I.7.6	<i>Odbiór Etapu/Dokumentacji/Końcowy</i>17
I.7.7	<i>Dostawa i instalacja oprogramowania standardowego</i>17
I.7.8	<i>Dostawa, instalacja, konfiguracja i wdrożenie Oprogramowania aplikacyjnego</i>17
I.7.9	<i>Testy</i>18
I.7.10	<i>Dodatkowe zobowiązania Wykonawcy</i>18
ROZDZIAŁ II.SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA	20
II.1	DOSTAWA I WDROŻENIE OPROGRAMOWANIA NARZĘDZIOWEGO I INFRASTRUKTURY SERWEROWEJ20
II.1.1	<i>Serwer aplikacyjny 1 szt.</i>23
II.1.2	<i>Serwer Bazodanowy – 1 sztuka</i>25
II.1.3	<i>Macierz – 2 sztuki</i>28
II.1.4	<i>Pamięć masowa – 1 sztuka</i>29
II.1.5	<i>Przełączniki FC– 2 sztuki</i>30
II.1.6	<i>Przełącznik rdzeniowy sieci LAN – 2 sztuki</i>30
II.1.7	<i>Przełącznik dostępowy sieci LAN typ 1 bez PoE - 4 sztuki</i>34
II.1.8	<i>Przełącznik dostępowy sieci LAN typ 2 z obsługą PoE - 4 sztuki</i>36
II.1.9	<i>Kompletny Punkt sieci bezprzewodowej wraz z dedykowanym zestawem montażowym</i>39
II.1.10	<i>Oprogramowanie do zarządzania siecią – licencje na 30 urzędzeń</i>45
II.1.11	<i>Oprogramowanie do wirtualizacji – 1 komplet</i>48
II.1.12	<i>Oprogramowanie do backupu – 1 komplet</i>54
II.1.13	<i>Baza danych – 2 szt.</i>55
II.2	WDROŻENIE OPROGRAMOWANIA SZPITALNEGO SYSTEMU INFORMATYCZNEGO SSI I EUSŁUG60
II.2.1	<i>Wymogi dotyczące interoperacyjności lub migracji dla oferowanego SSI</i>60
II.2.2	<i>Dostępność dostarczanego rozwiązania</i>60
II.2.3	<i>Wykaz posiadanych licencji</i>61
II.2.4	<i>Oprogramowanie aplikacyjne – wymagania ogólne</i>61
II.3	EUSŁUGI.....65
II.4	DOSTAWA I WDROŻENIE SILNIKA BAZY DANYCH WRAZ Z ZASILANIEM DANymi Z OBECNEJ POSIADANEJ PRZEZ ZAMAWIAJĄCEGO BAZY DANYCH ADAPTIVE SERVER ENTERPRISE/15.5/EBF66
II.4.1	<i>Baza danych – wymagania ogólne</i>66
II.4.2	<i>Dane w systemie HIS</i>66
II.4.3	<i>Interfejsy komunikacyjne</i>68
II.4.4	<i>Opis stanu bieżącego</i>68
II.4.5	<i>Zakres i przedmiot zasilenia danymi bazę danych</i>70
II.4.6	<i>Przenoszenie danych (migracja)</i>71
II.4.7	<i>Przebieg procesu migracji</i>73
II.4.8	<i>Asysta techniczna w procesie migracji produkcyjnej</i>76
II.4.9	<i>Testy</i>77
II.4.10	<i>Specyficzna procedura odbioru części związanej z migracją danych</i>82
II.4.11	<i>Warunki przeniesienia danych</i>84
II.4.12	<i>Instruktaże</i>84
ROZDZIAŁ III. GWARANCJA	87
III.1	USŁUGI GWARANCYJNE88
III.2	POZOSTAŁE USTALENIA:92

Rozdział I. Założenia początkowe oraz wymagania ogólne

I.1 Wprowadzenie

W projekcie „Wprowadzenie nowoczesnych e-usług w podmiotach leczniczych nadzorowanych przez Ministra Zdrowia” bierze udział 52 partnerów oraz lider projektu.

Realizacja przedmiotowego Projektu docelowo pozwoli wspomóc przygotowanie placówek ochrony zdrowia, które są odbiorcami Projektu, do prowadzenia dokumentacji medycznej w postaci elektronicznej oraz pozwoli na wymianę danych zawartych w elektronicznej dokumentacji medycznej, zaś wdrażane e-usługi zostały zidentyfikowane jako plasujące się wśród najbardziej oczekiwanych przez pacjentów¹.

I.2 Cel projektu

Celem głównym Projektu jest umożliwienie efektywnego świadczenia e-usług publicznych przez podmioty lecznicze. Podmioty biorące udział w Projekcie zrealizują dostosowanie systemów informatycznych części białej (HIS) do gromadzenia, przetwarzania oraz udostępniania elektronicznej dokumentacji medycznej (EDM) oraz świadczenia usług elektronicznych indywidualnie w każdym podmiocie leczniczym. Wymagać to będzie rozbudowy i/lub dostosowania obecnych systemów informatycznych HIS w podmiotach leczniczych uczestniczących w realizacji projektu, w zakresie wymaganym do świadczenia usług i funkcji planowanych w ramach Projektu. Ze względu na różny stan informatyzacji poszczególnych podmiotów leczniczych, zakres dostosowania systemów uwzględnia indywidualne potrzeby tych podmiotów niezbędne do zakresu Projektu i powoduje rozbudowę istniejących rozwiązań lokalnych. W wyniku realizacji Projektu każdy z podmiotów będzie gotowy do świadczenia poniższych e-usług i funkcjonalności:

- przetwarzanie i wymiana Elektronicznej Dokumentacji Medycznej,
- e-Rejestracja,
- e-Zlecenia,
- e-Analizy.

Przewidywana jest także rozbudowa warstwy infrastrukturalno–systemowej poprzez dostawę komponentów i rozwiązań w obszarze sieciowym, sprzętowym oraz oprogramowania systemowego.

¹ Źródło: Raport: „E-zdrowie. Czego oczekują pacjenci?” wraz z infografiką: <https://mvpacjenci.org/raporty.html> (badania przeprowadzono czerwiec-lipiec 2017r).

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 późn. zm), co najmniej w zakresie opisanym w dokumentach: „Opis usług biznesowych Systemu P1 wykorzystywanych w systemach usługodawców”, „Opis funkcjonalny Systemu P1 z perspektywy integracji systemów zewnętrznych” opublikowanych przez CSIOZ oraz „Minimalne wymagania dla systemów usługodawców (<https://www.gov.pl/web/zdrowie/minimalne-wymagania-dla-systemow-uslugodawcow>) oraz dokumentacja integracyjna dla obszaru Zdarzeń Medycznych i Indeksów EDM.

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

- Zakresu funkcjonalnego Projektu P1 (system musi posiadać m.in. możliwość wystawiania recept elektronicznych oraz skierowań elektronicznych),
- Opisu funkcjonalnego Systemu P1 z perspektywy integracji systemów zewnętrznych,

Dokumenty te dostępne są na stronie internetowej CSIOZ, pod adresem: <http://csioz.gov.pl>.

Wykonawca zobowiązany jest do zapewnienia integracji z węzłem krajowym identyfikacji elektronicznej. Wykonawca zobowiązany jest do dostarczenia puli licencji niezbędnych do integracji z węzłem krajowym w zakresie poprawnego działania całego przedmiotu zamówienia.

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

- System P1 dostępny będzie dla odpowiednio zarejestrowanych w CSIOZ systemów usługodawców i systemów regionalnych wyłącznie poprzez standardowe interfejsy Web Services. Wymagane jest dwustronne uwierzytelnianie systemów nawiązujących komunikację, a także podpisywanie komunikatów certyfikatem dostarczonym bądź wskazanym przez CSIOZ.
- Komunikaty przesyłane do P1 powinny być podpisane elektronicznie przez system komunikujący się z Systemem P1 certyfikatem wydanym przy zakładaniu konta usługodawcy (rejestrowaniu systemu). Wymagania w zakresie rodzaju stosowanego certyfikatu mogą ulec zmianie w wyniku wejścia w życie Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (rozporządzenie eIDAS) oraz/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 CSIOZ.

- W przypadku rejestru (indeksu) Elektronicznej Dokumentacji Medycznej – obowiązuje EDMiZM publikowany przez CSIOZ.
- Zgoda pacjenta na udostępnienie jego dokumentacji medycznej – funkcjonalność ta jest wymagana i powinna być zgodna z modelem dokumentu zgody oraz modelami interfejsów pozwalających na wnioskowanie o zgodę, które zostaną opublikowane przez CSIOZ.
- Wymiana Elektronicznej Dokumentacji Medycznej (dalej: EDM) – funkcjonalność ta jest wymagana i powinna być zgodna z modelem wniosku i dokumentu udostępnienia oraz modelami interfejsów, które zostaną opublikowane przez CSIOZ.

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

- Prowadzenie i wymiana Elektronicznej Dokumentacji Medycznej (EDM), w tym indywidualnej dokumentacji medycznej (wewnętrznej 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 CSIOZ – Polską Implementacją Krajową HL7 CDA (tzw. IG).
- Szpitalny System Informatyczny powinien uwzględniać funkcjonalności dotyczące prowadzenia repozytorium EDM (z obsługą przechowywania EDM) oraz uwzględniać rozwiązania zapewniające wymianę EDM pomiędzy repozytorium Zamawiającego, a Platformą P1. Platforma P1 będzie zawierała katalog EDM, w którym znajdować się będą informacje o EDM tworzonym i przechowywanym u Zamawiającego.
- Repozytorium EDM powinno realizować, co najmniej usługę przyjmowania, archiwizacji i udostępniania EDM zgodnej z HL7 CDA, a w przypadku repozytoriów badań obrazowych, przyjmowania, archiwizacji i udostępniania obiektów DICOM.

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. Rozwiązania muszą pozwalać na gromadzenie, przetwarzanie i analizowanie danych i informacji w obszarach objętych wdrożeniem, na bazie tych danych musi istnieć możliwość wytwarzania prawidłowej, kompletnej, ujętej w obowiązujących przepisach prawa dokumentacji (dokumenty, raporty, wykazy, oświadczenia, zaświadczenia itp.).

I.5 Ogólny opis przedmiotu zamówienia

Przedmiot zamówienia niniejszego postępowania przetargowego obejmuje dostawę i wdrożenie Infrastruktury Serwerowej wraz z oprogramowaniem systemowym i narzędziowym oraz wdrożenie oprogramowania systemu szpitalnego będącego w posiadaniu Zamawiającego wraz z usługą migracji danych do jednego wspólnego środowiska bazodanowego.

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

- Infrastruktura serwerowa w zakresie:

POZ. SOPZ	OPIS	ILOŚĆ SZTUK
ROZDZIAŁ II.1	INFRASTRUKTURA SERWEROWA	
II.1.1	Serwer aplikacyjny	1
II.1.2	Serwer bazodanowy	1
II.1.3	Macierz dyskowa	2
II.1.4	Pamięć masowa	1
II.1.5	Przełącznik FC	2
II.1.6	Przełączniki rdzeniowy sieci LAN	2
II.1.7	Przełącznik dostępowy sieci LAN typ 1	4
II.1.8	Przełącznik dostępowy sieci LAN typ 2	4
II.1.9	Kompletny punkt sieci bezprzewodowej AP WIFI	15

- Oprogramowanie systemowe i narzędziowe w zakresie:

POZ. SOPZ	OPIS	ILOŚĆ
ROZDZIAŁ II.2	OPROGRAMOWANIE SYSTEMOWE I NARZĘDZIOWE	
II.I.11	Oprogramowanie wirtualizacyjne	1 komplet
II.I.12	Oprogramowanie do backup	1 komplet
II.I.10	Licencje systemu zarządzania siecią oraz urządzeniami sieciowymi	30
II.I.13	Oprogramowanie bazodanowe	2

2) Wdrożenie oprogramowania Szpitalnego Systemu Informatycznego SSI i eUsług:

POZ. SOPZ	OPIS
ROZDZIAŁ II.3	SZPITALNY SYSTEM INFORMATYCZNY
II.2.5	HIS – część medyczna – wdrożenie eUsług i migracja bazy danych
II.2.6	Instruktaże stanowiskowe

1. Przedmiot zamówienia musi być dostarczany, wdrożony i zainstalowany w całości do siedziby Zamawiającego.
2. Wszystkie dostarczane:
 - Produkty (rozumiane jako elementarny efekt działań/prac/dostaw objętych całym zakresem Przedmiotu Zamówienia wykonywanych przez Wykonawcę podczas realizacji Umowy w poszczególnych Etapach).
 - Komponenty (rozumiane jako integralna część dostawy i wdrożenia Przedmiotu Zamówienia, składający się przynajmniej z jednego Produktu lub wielu Produktów powiązanych ze sobą merytorycznie) podlegają usługom projektowania, dostaw, instalacji, konfiguracji i wdrożenia.
3. Usługi projektowania, instalacji, konfiguracji i wdrożenia Wykonawca przeprowadzi zgodnie z zapisami 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, niniejszymi 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 Załączniku nr 3 do SIWZ 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 i 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 i elementy, które są niezbędne do prawidłowego funkcjonowania całości. W przypadku, gdy w trakcie realizacji Przedmiotu Zamówienia okaże się, że brakuje jakiegokolwiek urządzenia lub elementu, którego brak spowoduje nieprawidłowe funkcjonowanie całości Przedmiotu Zamówienia, Wykonawca dostarczy je na własny koszt.
7. Zamawiający wymaga, aby zaoferowane rozwiązanie 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.

I.6 Termin realizacji Przedmiotu Zamówienia

Termin realizacji całości Przedmiotu zamówienia wynosi 270 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 przeprowadzić dostawy Przedmiotu Zamówienia w dokładnych terminach i godzinach uzgodnionych z Zamawiającym.
5. W przypadku dostarczania Infrastruktury Sprzętowej musi być ona oznakowana w taki sposób, aby możliwa była identyfikacja systemowa zarówno produktu jak i producenta, sprzęt musi pochodzić z oficjalnych kanałów dystrybucji producentów i zostać dostarczony w oryginalnych opakowaniach fabrycznych.
6. Wdrożenie należy rozumieć jako szereg uporządkowanych i zorganizowanych działań mających na celu wykonanie Przedmiotu Zamówienia.
7. Realizacja przedmiotu zamówienia będzie realizowana w ramach powołanych do tego celu struktur organizacyjnych po stronie Wykonawcy.
8. W ramach wdrożenia Wykonawca przygotowuje informacje na temat struktury organizacyjnej Zespołu Wykonawcy zajmującej się realizacją Przedmiotu Zamówienia, w ramach której muszą zostać powołane minimum następujące role:
 - a. Kierownik Projektu ze strony Wykonawcy,
 - b. Zespół Wdrożeniowy ze strony Wykonawcy
9. 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 przekaze Zamawiającemu wykaz numerów telefonów kontaktowych do kluczowych osób biorących udział w realizacji Przedmiotu Zamówienia po stronie Wykonawcy.
10. W skład operacyjnego Kierownictwa wchodzi Kierownik Projektu ze strony Zamawiającego oraz Kierownik Projektu ze strony Wykonawcy. Wykonawca i Zamawiający są zobowiązani do wskazania osób pełniących role Kierownika Projektu.
11. Obowiązki Kierownika Projektu ze strony Wykonawcy:

- a. Wyznaczenie osób upoważnionych do realizacji przedmiotu umowy.
- b. Lista osób upoważnionych zostanie przekazana Kierownikowi Projektu ze strony Zamawiającego bezzwłocznie po podpisaniu umowy oraz bezzwłocznie po każdej zmianie osób upoważnionych.
- c. Nadzór nad czynnościami realizowanymi, w ramach realizacji przedmiotu umowy, przez osoby upoważnione o których mowa w pkt. 1, w szczególności w zakresie zgodności z postanowieniami umowy.
- d. Tworzenie planów etapów i ewentualnych planów awaryjnych.
- e. Tworzenie harmonogramu projektu.
- f. Zgłaszanie, zatwierdzanie gotowości do odbioru usług Kierownikowi Projektu ze strony Zamawiającego.
- g. Zgłaszanie potrzeby konsultacji i doradztwa w zakresie realizacji projektu.
- h. Nadzór i kontrola realizacji prac i zobowiązań zgodnie z uzgodnionymi terminami.
- i. Prowadzenie i archiwizowanie dokumentacji zdarzeń i czynności wykonanych w ramach realizacji umowy, pozwalających na ustalenie faktów związanych m.in. ze zlecaniem, odbiorem i rozliczeniem usług.
- j. Zapewnienie odpowiedniego zastępstwa na czas swojej nieobecności z poinformowaniem Kierownika Projektu ze strony Zamawiającego.
- k. Przedkładanie informacji Kierownikowi Projektu ze strony Zamawiającego zgodnie z jego potrzebami.
- l. Przedkładanie wniosków, sugestii i propozycji Kierownikowi Projektu ze strony Zamawiającego zgodnie z potrzebami.
- m. Realizowanie we współpracy z Kierownikiem ze strony Zamawiającego wszystkich zadań związanych z procesem zarządzania Projektem.
- n. Kontrola zakresu Projektu.
- o. Zarządzanie ryzykiem.
- p. Wspólna z Kierownikiem Projektu ze strony Zamawiającego kontrola terminowej i zgodnej z budżetem realizacji Projektu, w szczególności w obszarach prac wykonywanych przez pracowników Wykonawcy.
- q. Wspólne z Kierownikiem Projektu ze strony Zamawiającego rozwiązywane istotnych kwestii pojawiających się podczas prac projektowych; nadzór nad Liderami Zespołów Projektowych.
- r. Koordynacja przeprowadzenia odbioru prac w Projekcie. W przypadku powstania kwestii spornych między stronami zaangażowanymi w realizację Projektu Kierownik powinien być stroną rozstrzygającą o najlepszym rozwiązaniu.

12. Wykonawca zorganizuje prace tak, aby w maksymalnym stopniu nie zakłócać ciągłości funkcjonowania prac u Zamawiającego.
13. 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.
14. 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, Dokumentacją PZ), która składa się z nw. zakresów:
 - a) Harmonogram Wdrożenia.
 - b) Dokumentacja Analizy Przedwdrożeniowej (DAP).
 - c) Dokumentacja Powykonawcza.
2. Dokumentacja 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 (dalej zwanych SIWZ) wraz z załącznikami, będą stanowiły podstawę do weryfikacji realizacji przedmiotu zamówienia w trakcie odbiorów.
3. Dokumentacja podlega uzgadnianiu i akceptacji Zamawiającego. Akceptacja Harmonogramu wdrożenia i DAP warunkuje rozpoczęcie prac Wykonawcy.
4. Dokumentacja Analizy Przedwdrożeniowej DAP wraz z harmonogramem wdrożenia zostaną opracowane w oparciu o wymagania określone w niniejszym SOPZ.

I.7.3 **Harmonogram wdrożenia**

Wykonawca zobowiązany jest opracować na podstawie SIWZ wraz z załącznikami, szczegółowy harmonogram wdrożenia. Harmonogram należy przedstawić Zamawiającemu w terminie do 30 dni od dnia podpisania Umowy.

I.7.4 Analiza Przedwdrożeńiowa

1. Analiza przedwdrożeńiowa, którą należy rozumieć jako zakres czynności do wykonania przez Wykonawcę mający na celu analizę środowiska biznesowego i informatycznego Zamawiającego. W wyniku przeprowadzenia Analizy przedwdrożeńiowej Wykonawca przedstawi Zamawiającemu Dokumentację analizy przedwdrożeńiowej (zwana dalej DAP), na podstawie, której będzie realizowany organizacyjnie i technicznie Przedmiot Zamówienia. DAP będzie podlegała uzgodnieniu i akceptacji Zamawiającego.
2. W zakresie analizy przedwdrożeńiowej Wykonawca zobowiązany będzie co najmniej do:
 - Przeprowadzenia audytu istniejącego rozwiązania celem identyfikacji i inwentaryzacji konfiguracji elementów niestandardowych systemu HIS użytkowanego przez Zamawiającego w szczególności:
 - a) Raportów
 - b) Wydruków
 - c) Formularzy
 - d) Integracji z innymi systemami
 - e) Bieżącej konfiguracji systemu HIS
 - f) Konfiguracji procedur backupu systemu HIS
 - Wszystkie elementy wynikające z audytu zostaną uwzględnione w planie migracji systemu. Warunkiem zaakceptowania planu migracji, a następnie jego realizacji jest odtworzenie istniejącej funkcjonalności [mowa o zakresie funkcjonalnym, obsłudze procesu] obecnego systemu również w zakresie elementów niestandardowych wymienionych w pkt a-f. Zamawiający zastrzega sobie prawo rezygnacji z przenoszenia wybranych obszarów danych. Zamawiający potwierdzi zakres przenoszonych obszarów po wykonaniu audytu instalacji na etapie analizy przedwdrożeńiowej. Decyzja w tym zakresie jest wyłączną kompetencją Zamawiającego.
 - Opracowania planu migracji – Plan migracji będzie opisywał proces migracji danych z obecnie użytkowanej bazy do wydajnej bazy danych i będzie zawierał minimum następujące elementy:
 - a) Wskazanie zadań leżących po stronie Wykonawcy,
 - b) Wskazanie zadań leżących po stronie Zamawiającego,
 - c) Szczegółowy harmonogram planowanych prac ze szczególnym uwzględnieniem sytuacji w której obecnie użytkowany system będzie niedostępny,
 - d) Opracowanie projektu technicznego migracji danych systemu HIS,

3. Dokumentacja Analizy Przedwdrożeniowej DAP powinna zawierać w szczególności:

SKŁAD DAP
SSI
- wykaz oraz szczegółowy opis i harmonogram wdrożenia SSI i eUsług
- architekturę SSI i eUsług
- analizę przedwdrożeniową procesu migracji i plan migracji danych oraz opis sposobu migracji
- przygotowanie planu instalacji Infrastruktury serwerowej
- przygotowanie planu instalacji macierzy dyskowych
- jednoznacznie określone założenia integracji z innymi systemami informatycznymi, które posiada Zamawiający
- plan pracy na dalsze 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 i eUsług
- 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 i eUsług
ZARZĄDCZE
- plan i sposób komunikacji Stron
INFRASTRUKTURA SERWEROWA
- 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
- lista Komponentów, które będą podlegały osobnym odbiorom – jeżeli dotyczy

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:

1) Wymogi ogólne:

1. Pełna charakterystyka licencjonowania wszystkich elementów aplikacji i środowiska.
2. Opis architektury technicznej:
 - wyszczególnienie oraz opis powiązań wszystkich komponentów sprzętowych, systemowych i aplikacyjnych występujących lub wymaganych do poprawnej pracy aplikacji zgodnie z wymaganiami wydajności, funkcjonalności i bezpieczeństwa (minimalny, maksymalny, rekomendowany),
 - dla komponentów innych dostawców, należy dokładnie określić wykorzystywane i dopuszczalne wersje – jeżeli dotyczy;
3. Konfiguracja musi obejmować wszystkie urządzenia wdrożone, zainstalowane w ramach budowy systemu IT.
4. Mapa i opis Interface'ów.
 - interfejsy muszą zawierać szczegółowy opis techniczny, w szczególności zawierać informację o: typie interfejsu, wykorzystywanych protokołach, portach sieciowych, strukturze interfejsu, itp. oraz o zakresie wymiany danych i sposobie kontroli prawidłowości działania.
5. Procedury lub instrukcje instalacji, reinstalacji, deinstalacji oraz aktualizacji.
 - szczegółowy opis postępowania w przypadku tworzenia lub zmian w środowisku; jeśli wykorzystywane są procedury innych dostawców dla standardowych komponentów (np. baz danych) wystarczy wskazać w dokumentacji szczegółowe odniesienie do procedur standardowych właściwych dla tych komponentów.
6. Dokumentacja administracyjna związana z poprawną eksploatacją
 - opis (w postaci procedur lub instrukcji) wszystkich rutynowych czynności administracyjnych dla aplikacji i systemu informatycznego (dziennych, tygodniowych, miesięcznych itp.) oraz działań pozwalających na utrzymanie wymaganej dostępności, wydajności i bezpieczeństwa,
 - wymagane jest dostarczenie poprawnych inicjalnych sekwencji realizowanych czynności administracyjnych i utrzymaniowych i zasad ich aktualizacji i budowy; opis zasad pielęgnacji i utrzymania aplikacji. Procedury administracyjne powinny w szczególności zawierać informacje o okresowych zadaniach, które muszą być wykonane przez administratora, np. weryfikacja zajętości przestrzeni tabel, konieczność wykonywania analizy tabel, czyszczenia logów, itp.

7. Procedury standardowe:

- opis możliwości stosowania standardowych procedur poprawnej eksploatacji dla rozwiązań wspierających (sprzętowych lub aplikacyjnych).

8. Dokumenty z testów:

- plan testów, scenariusze testowe i protokoły z testów akceptacyjnych, wydajnościowych, testów operacji administratora technicznego oraz testów bezpieczeństwa w tym ciągłości działania (przełączanie, odtwarzanie, weryfikacja poprawności).

9. Dokumentacja wdrożeniowa:

- dokumentacja powdrożeniowa: zawiera szczegółowy opis wykonanych czynności instalacyjnych oraz konfiguracyjnych wszystkich komponentów systemu;
- dokumentacja parametryzacji: wyszczególnienie wartości wszystkich ustawionych parametrów użytkowych zarówno samej aplikacji jak i pozostałych komponentów systemu, parametry systemu operacyjnego oraz parametry sprzętu, w tym konfiguracji środowiska produkcyjnego (serwery baz danych, serwery aplikacji, inne zastosowane);
- dokumentacja uruchomieniowa: opisuje wszystkie istotne kroki (czynności) wykonane w celu pierwszego uruchomienia aplikacji/systemu, w tym opis migracji/konwersji danych, testy uruchomieniowe;

10. Zalecenia:

- opis zasad i zaleceń strojenia aplikacji.

11. Instrukcje obsługi i instrukcje użytkownika dla wersji dostarczonego oprogramowania z podziałem na poszczególne moduły.

12. W zakresie obszarów administratora dokumentacja powinna zawierać dodatkowo co najmniej:

- opis podstawowych ról użytkowników i zasad ich kreowania
- opis zarządzania uprawnieniami użytkownika i tworzenia profili;
- lista dostępnych uprawnień użytkownika wraz z opisem efektu w zakresie dostępu do danych w SSI;
- opis zarządzania autoryzacją i autentykacją użytkowników

2) Wymogi szczegółowe:

1. Opis aplikacji i konfiguracji aplikacji/systemu.

- opis musi obejmować ogół oprogramowania wdrożonego, zainstalowanego w ramach budowy systemu IT,
- opis musi zawierać opis systemu lub systemów informatycznych, zawierający wykaz programów, procedur lub funkcji, w zależności od struktury oprogramowania, wraz z opisem algorytmów i parametrów oraz programowych zasad ochrony danych, w tym w

szczegółności metod zabezpieczania dostępu do danych i systemu ich przetwarzania, sposobu komunikacji pomiędzy systemami, zakresu wymienianych danych i sposobu ich szyfrowania,

- konfiguracja musi obejmować wersję aplikacji, pełen zestaw parametrów konfiguracyjnych aplikacji wraz z opisem użycia, katalogi instalacyjne, położenie plików konfiguracyjnych, położenie plików logów, położenie i opis innych kluczowych plików i katalogów, itp.

2. Opis struktur baz danych

- opis wykorzystywanych struktur danych musi w szczególności zawierać: listę tabel bazy danych wraz z opisem pól, formaty danych, itp., kryteria walidacji danych wejściowych, opis zmiennych konfiguracyjnych;

3. Procedury eksploatacji.

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

4. Procedury backupowe:

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

I.7.6 Odbiór Etapu/Dokumentacji/Końcowy

1. Odbiory Etapów/Dokumentacji będą się odbywać po zakończeniu określonych prac danego Etapu/Dokumentacji.
2. Odbiór końcowy Przedmiotu Zamówienia ma na celu potwierdzenie wykonania wszystkich zadań wynikających z Umowy, w tym odebrania wszystkich Komponentów i Etapów oraz dostarczenia wymaganej zamówieniem Dokumentacji.
3. Odbiory będą odbywać się zgodnie z zapisami w Umowie stanowiącej załącznik nr 9 do SIWZ.

I.7.7 Dostawa i instalacja oprogramowania standardowego

4. Oprogramowanie standardowe rozumiane jako oprogramowanie dostarczone i zainstalowane na Infrastrukturze serwerowej oraz sieciowej posiadanej przez Zamawiającego lub dostarczanej zgodnie z Umową stanowiącą załącznik nr 9 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.
5. Dostawa i instalacja zostaną wykonane w lokalizacjach zgodnych z instalacją urządzeń u Zamawiającego zgodnie z Harmonogramem wdrożenia.
6. 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 – baza danych
 - eUsługi
2. Dostawa i instalacja mają 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 oczekiwaniami konfiguracyjnymi samego procesu wdrażania (w zakresie opisanych w OPZ wymagań funkcjonalnych).

4. Oprogramowanie aplikacyjne musi zostać zainstalowane przez Wykonawcę w szczególności z wykorzystaniem Sprzętu dostarczanego przez Wykonawcę i w środowiskach informatycznych Zamawiającego. Oprogramowanie aplikacyjne musi zostać zainstalowane i skonfigurowane w sposób kompleksowy na wszystkich stanowiskach komputerowych Zamawiającego.
5. Zamawiający na potrzeby realizacji przedmiotu zamówienia przewidział infrastrukturę serwerową i oprogramowanie o parametrach wskazanych w rozdziale II niniejszego SOPZ.

I.7.9 Testy

1. W ramach postępowania zostaną przeprowadzone wszystkie testy opisane w Dokumentacji. Celem testów jest weryfikacja przez Zamawiającego czy wszystkie prace wykonane w trakcie realizacji Przedmiotu Zamówienia zostały wykonane prawidłowo i zgodnie z założeniami funkcjonalnymi i jakościowymi. Testy będą przeprowadzane przez Wykonawcę przy współdziałaniu Zamawiającego jak i wskazanych przez Zamawiającego osób i podmiotów zewnętrznych.
2. Pozytywne zakończenie testów wraz z usunięciem wskazanych Wad jest niezbędne, aby dla poszczególnych Komponentów oraz całego Przedmiotu Zamówienia dokonać odbiorów w ramach poszczególnych Etapów i Odbioru końcowego.
3. Zamawiający ma prawo do weryfikacji należytego wykonania Umowy dowolną metodą, w tym także z wykorzystaniem opinii zewnętrznego audytora. W szczególności uzgodnienie określonych scenariuszy testowych nie wyklucza prawa do weryfikacji prac innymi testami i scenariuszami.
4. Zamawiający w końcowej fazie wdrożenia oczekuje realizacji przez Wykonawcę testów bezpieczeństwa. Testy obejmować będą swym zakresem:
 - a) Testy bezpieczeństwa aplikacji wytworzonych i dostarczonych w ramach projektu wskazanych przez Zamawiającego na etapie Analizy przedwdrożeniowej;
 - b) Testy poprawności konfiguracji i parametryzacji sprzętu serwerowego oraz sprzętu sieciowego aktywnego na styku komunikacji z zewnętrzną siecią.
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 Kończącym 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 załącznikiem nr 9 do SIWZ.

3. Dokonanie z Zamawiającym wszelkich koniecznych ustaleń mogących wpływać na zakres i sposób realizacji Przedmiotu Zamówienia oraz ciągła współpraca z Zamawiającymi 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 narzędziowego 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 (Systemu Komunikacyjnego) Zamawiającego.
3. Wykonawca jest zobowiązany dokonać montażu dostarczonej Infrastruktury Serwerowej oraz oprogramowania w miejscach wskazanych przez Zamawiającego.
4. Wszystkie elementy Infrastruktury serwerowej powinny zostać zamontowane w szafach 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 / łąt systemowych po stronie serwerów
 - Przygotowanie szczegółowej koncepcji konfiguracji dysków macierzy odzwierciedlającej potrzeby biznesowe
 - Zestawienie zakupionego oprogramowania
 - Propozycja testów odbiorczych
 - Implementacja zgodna z projektem:
 - Instalacja sprzętowa
 - Aktywacja zakupionego oprogramowania
 - Konfiguracja replikacji synchronicznej
 - 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 / łąt 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 łą 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 łą 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 łą systemu operacyjnego (ang. Patch Management)
 - Zestawienie wersji zainstalowanego oprogramowania
7. Po zakończonym montażu Wykonawca przekaze Zamawiającemu wszystkie hasła dostępowe do kont „super użytkowników” oraz dokumentację do wszystkich oferowanych urządzeń, oprogramowania narzędziowego (systemowego, bazodanowego, wirtualizacyjnego, backupowego itd.) wraz z dokumentami potwierdzającymi nabycia dla Zamawiającego licencji (nie dotyczy samego systemu SSI) oraz nośnikami danych zawierającymi zainstalowane oprogramowanie (o ile dostarcza je producent). Wykonawca wykona również instruktaże użytkowe dla wskazanego przez Zamawiającego administratora, z zakresu konfiguracji, obsługi i prawidłowej eksploatacji zainstalowanego Sprzętu ze szczególnym uwzględnieniem obsługi i zaawansowanego zarządzania macierzą zewnętrzną, w środowisku Zamawiającego.
8. W całym okresie trwania Umowy Wykonawca zobowiązany jest zapewnić 3 miesięczne wsparcie i możliwość prowadzenia konsultacji w zakresie administracji zaoferowanym sprzętem oraz

dostarczonym oprogramowaniem narzędziowym (systemowym, wirtualizacyjnym, backup-owym i bazodanowym) z osobami wskazanymi przez Wykonawcę.

II.1.1 Serwer aplikacyjny 1 szt.

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

WYMAGANE MINIMALNE PARAMETRY TECHNICZNE	
Obudowa	Obudowa Rack o wysokości max 2U z możliwością instalacji min. 12 dysków 3.5" Hot-Plug wraz z kompletem szyn umożliwiających montaż w szafie rack.
Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocessorowych
Procesor	Zainstalowany jeden procesor szesnastordzeniowy x86 (niedopuszczalne jest dostarczenie serwera z zainstalowanymi 2 procesorami) umożliwiający osiągnięcie wyniku min. 180 punktów w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla dwóch procesorów.
RAM	256GB DDR4 RDIMM 2666MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Zabezpieczenia pamięci RAM	Memory Rank Sparing
Gniazda PCI	min. 4 aktywne sloty Gen. 3
Interfejsy sieciowe/FC	Zainstalowane dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT. Zainstalowane dodatkowe dwie karty dwuportowe 10GbE w standardzie BaseT. Zainstalowane dodatkowo dwie karty FC dwuportowe w standardzie minimum 16Gb/s wraz z wkładkami.
Dyski twarde	Zainstalowane 2 x 480GB SSD Zainstalowany wewnętrzny moduł dedykowany dla hypervisora wirtualizacyjnego, wyposażony w 2 jednakowe nośniki typu flash o pojemności minimum 32GB z możliwością konfiguracji zabezpieczenia RAID 1 z poziomu

	BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnek na dyski twarde.
Kontroler RAID	Sprzętowy kontroler dyskowy, umożliwiający konfiguracje poziomów RAID: 0, 1, 5, 10, 50.
Wbudowane porty	min. 2 porty USB 2.0 oraz 2 porty USB 3.0, 2 porty wideo (1 na przednim panelu obudowy VGA lub DisplayPort, drugi na tylnym VGA), min. 1 port RS232
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug maksymalnie 750W.
Bezpieczeństwo	Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. TPM 2.0
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające: <ul style="list-style-type: none"> • zdalny dostęp do graficznego interfejsu Web karty zarządzającej • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera) • szyfrowane połączenie (SSLv3) oraz autentykację i autoryzację użytkownika • możliwość podmontowania zdalnych wirtualnych napędów • wirtualną konsolę z dostępem do myszy, klawiatury • wsparcie dla IPv6 • wsparcie dla SNMP; IPMI2.0, VLAN tagging, Telnet, SSH • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer • integracja z Active Directory • możliwość obsługi przez dwóch administratorów jednocześnie • wsparcie dla dynamic DNS • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej • możliwość podłączenia lokalnego poprzez złącze RS-232

	<ul style="list-style-type: none"> • możliwość zarządzania bezpośredniego oraz poprzez złącze USB umieszczone na froncie obudowy.
Certyfikaty	<p>Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001. Serwer musi posiadać deklaracja CE.</p> <p>Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2012 R2, Windows Server 2016, Windows Server 2019.</p>
Warunki gwarancji	<p>Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta.</p> <p>W przypadku awarii dyski twarde pozostają własnością zamawiającego.</p>
Dokumentacja użytkownika	<p>Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</p> <p>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p>

II.1.2 Serwer Bazodanowy – 1 sztuka

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

Wymagane minimalne parametry techniczne	
Obudowa	Obudowa Rack o wysokości max 2U z możliwością instalacji min. 12 dysków 3.5" Hot-Plug wraz z kompletem szyn umożliwiających montaż w szafie rack.
Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocessorowych
Procesor	Zainstalowany jeden procesor szesnastordzeniowy x86 (niedopuszczalne jest dostarczenie serwera z zainstalowanymi 2 procesorami) umożliwiający osiągnięcie wyniku min. 180 punktów w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla dwóch procesorów.

RAM	256GB DDR4 RDIMM 2666MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Zabezpieczenia pamięci RAM	Memory Rank Sparing
Gniazda PCI	min. 4 aktywne sloty Gen. 3
Interfejsy sieciowe/FC	Zainstalowane dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT. Zainstalowane dodatkowe dwie karty dwuportowe 10GbE w standardzie BaseT Zainstalowane dodatkowo dwie karty FC dwuportowe w standardzie minimum 16Gb/s obsadzone wkładkami.
Dyski twarde	Zainstalowane 2 x 480GB SSD Zainstalowany wewnętrzny moduł dedykowany dla hypervisora wirtualizacyjnego, wyposażony w 2 jednakowe nośniki typu flash o pojemności minimum 32GB z możliwością konfiguracji zabezpieczenia RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnek na dyski twarde.
Kontroler RAID	Sprzętowy kontroler dyskowy, umożliwiający konfiguracje poziomów RAID: 0, 1, 5, 10, 50.
Wbudowane porty	min. 2 porty USB 2.0 oraz 2 porty USB 3.0, 2 porty wideo (1 na przednim panelu obudowy VGA lub DisplayPort, drugi na tylnym VGA), min. 1 port RS232
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug maksymalnie 750W.
Bezpieczeństwo	Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. TPM 2.0
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające: <ul style="list-style-type: none"> • zdalny dostęp do graficznego interfejsu Web karty zarządzającej • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera) • szyfrowane połączenie (SSLv3) oraz autentykacje i autoryzację użytkownika • możliwość podmontowania zdalnych wirtualnych napędów

	<ul style="list-style-type: none"> • wirtualną konsolę z dostępem do myszy, klawiatury • wsparcie dla IPv6 • wsparcie dla SNMP; IPMI2.0, VLAN tagging, Telnet, SSH • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer • integracja z Active Directory • możliwość obsługi przez dwóch administratorów jednocześnie • wsparcie dla dynamic DNS • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej • możliwość podłączenia lokalnego poprzez złącze RS-232 • możliwość zarządzania bezpośredniego oraz poprzez złącze USB umieszczone na froncie obudowy.
Certyfikaty	<p>Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2012 R2, Windows Server 2016, Windows Server 2019.</p>
Warunki gwarancji	<p>Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta. W przypadku awarii dyski twarde pozostają własnością zamawiającego.</p>
Dokumentacja użytkownika	<p>Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p>

II.1.3 Macierz – 2 sztuki

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

WYMAGANE MINIMALNE PARAMETRY TECHNICZNE	
Obudowa	Do instalacji w standardowej szafie RACK 19” rozwiązanie może zajmować maksymalnie 2U i pozwalać na instalację 12 dysków 3.5”.
Kontrolery	Dwa kontrolery RAID pracujące w układzie active-active posiadające łącznie minimum osiem portów FC 16Gb wraz z wkładkami 8xSFP+ FC16Gb.
Dyski	Zainstalowane 4 dyski NLSAS o pojemności 4TB oraz 5 dysków 1.92TB SSD SAS 12Gbps, możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych do łącznie minimum 264 dysków. Możliwość mieszania typów dysków w obrębie macierzy oraz pojedynczej półki.
Oprogramowanie/Funkcjonalności	Zarządzanie macierzą poprzez minimum przeglądarkę internetową, GUI oparte o HTML5. Powiadamianie mailem o awarii, umożliwiające maskowanie i mapowanie dysków. Macierz powinna zostać dostarczona z licencją umożliwiającą utworzenie minimum 512 LUN’ów oraz 1024 kopii migawkowych na całą macierz. Licencja zaoferowanej macierzy powinna umożliwiać podłączanie minimum 8 hostów bez konieczności zakupu dodatkowych licencji. Konieczne jest posiadanie automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane między różnymi typami dysków. Możliwość wykorzystania dysków SSD jako cache macierzy, możliwość rozbudowy pamięci cache do min. 4TB poprzez dyski SSD. Macierz musi posiadać funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie asynchronicznym.
Wsparcie dla systemów operacyjnych	Windows Server 2012 R2, Windows Server 2016, Red Hat Enterprise Linux (RHEL), SLES, Vmware ESXi.
Bezpieczeństwo	Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne.

<p>Warunki gwarancji dla macierzy</p>	<p>Trzy lata gwarancji producenta realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. W przypadku awarii dysków pozostają one własnością Zamawiającego.</p> <p>Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikro kodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji macierzy.</p> <ul style="list-style-type: none"> • Wszystkie naprawy gwarancyjne powinny być możliwe na miejscu. • Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu. <p>W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).</p>
<p>Dokumentacja użytkownika</p>	<p>Zamawiający wymaga dokumentacji w języku polskim lub angielskim</p>
<p>Certyfikaty</p>	<p>Macierz musi być wyprodukowana zgodnie z normą ISO 9001</p>

II.1.4 Pamięć masowa – 1 sztuka

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

WYMAGANE MINIMALNE PARAMETRY TECHNICZNE	
<p>Obudowa</p>	<p>Obudowa Rack o wysokości max 2U z możliwością instalacji min.12 dysków 3.5" wraz z kompletem szyn umożliwiających montaż w szafie rack.</p>
<p>Procesor</p>	<p>Minimum cztery rdzenie o taktowaniu bazowym 2,1 GHz.</p>
<p>RAM</p>	<p>16GB DDR4 UDIMM, na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 64GB pamięci RAM.</p>
<p>Porty</p>	<p>Min. 2x USB 3.0 Min. 4x USB 2.0</p>

	<p>Min. 4x RJ-45 1GbE</p> <p>Min. 2x 10GbE SFP+</p> <p>Min. 2 gniazda M.2 2280</p>
Zainstalowane Dyski	Min. 12x 6TB 3,5" 256MB cache dedykowane do urządzeń typu NAS
Obsługiwane Systemy plików	EXT4,EXT3,NTFS,HFS+
Obsługiwane poziomy RAID	<ul style="list-style-type: none"> • RAID 0 • RAID 1 • RAID 5 • RAID 6 • RAID 10 • RAID 50 • RAID 60
Obsługiwane protokoły sieciowe	SMB, NFS v3, iSCSI, HTTP, HTTPs, FTP, SNMP, Telnet, SSH
Zasilacze	Redundantne, Hot-Plug maksymalnie 350W.
Warunki gwarancji	<p>Trzy lata gwarancji.</p> <p>W przypadku awarii dysków pozostają one własnością Zamawiającego.</p>

II.1.5 Przelączniki FC– 2 sztuki

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

II.1.6 Przelącznik rdzeniowy sieci LAN – 2 sztuki

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

WYMAGANE MINIMALNE PARAMETRY TECHNICZNE	
1.	Przełącznik FC musi być wykonany w technologii FC 16 Gb/s i posiadać możliwość pracy portów FC z prędkościami 16, 8, 4 z funkcją autonegociacji prędkości.
2.	Przełącznik FC musi posiadać minimum 24 sloty na moduły FC. Wszystkie wymagane funkcje muszą być dostępne dla 24 portów FC przełącznika.
3.	Przełącznik musi być dostarczony wraz z minimum 24 modułami SFP FC 16 Gb/s.
4.	Rodzaj obsługiwanych portów: D_Port (ClearLink Diagnostic Port), E_Port, F_Port, M_Port (Mirror Port);
5.	Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) i szerokość 19" oraz zapewniać techniczną możliwość montażu w szafie 19".
6.	Przełącznik FC musi posiadać nadmiarowe wentylatory N+1 oraz redundantne zasilacze.
7.	Przełącznik FC musi być wykonany w tzw. architekturze „non-blocking” uniemożliwiającej blokowanie się ruchu wewnątrz przełącznika przy pełnej prędkości pracy wszystkich portów.
8.	Przełącznik musi posiadać mechanizm balansowania ruchu między grupami połączeń tzw. „trunk” oraz obsługiwać grupy połączeń „trunk” o różnych długościach.
9.	Przełącznik FC musi udostępniać usługę Name Server Zoning - tworzenia stref (zon) w oparciu bazę danych nazw serwerów.
10.	Przełącznik FC musi posiadać możliwość wymiany i aktywacji wersji firmware’u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia, bez wymogu ponownego uruchomienia urządzeń w sieci SAN.
11.	Przełącznik FC musi posiadać możliwość konfiguracji przez komendy tekstowe w interfejsie znakowym oraz przez przeglądarkę internetową z interfejsem graficznym.
12.	Przełącznik FC musi mieć możliwość instalacji jednomodowych SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 10km.
13.	Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC
14.	Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S v1.1 (powinien zawierać agenta SMI-S zgodnego z wersją standardu v1.1)
15.	Przełącznik FC musi zapewniać możliwość nadawania adresu IP dla zarządzającego portu Ethernet za pomocą protokołu DHCP
16.	Maksymalny dopuszczalny pobór mocy przełącznika FC to 80W
WYMAGANE MINIMALNE PARAMETRY TECHNICZNE	

17.	Przełącznik FC musi zapewniać możliwość dynamicznego aktywowania portów za pomocą zakupionych kluczy licencyjnych.
18.	Przełącznik FC musi zapewniać opóźnienie przy przesyłaniu ramek FC między dowolnymi portami nie większe niż 700ns.
19.	Przełącznik FC musi zapewniać sprzętową obsługę zoniingu na podstawie portów i adresów WWN
20.	Urządzenie musi wspierać mechanizm balansowania ruchem w połączeniach wewnątrz wielodomenowych sieci fabric w oparciu OXID.
21.	Możliwość wymiany w trybie „na gorąco”: minimum w odniesieniu do modułów portów Fibre Channel (SFP).
22.	Wsparcie dla N_Port ID Virtualization (NPIV). Obsługa co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika.
23.	Przełącznik FC musi mieć możliwość agregacji połączeń ISL między dwoma przełącznikami i tworzenia w ten sposób logicznych połączeń typu trunk.
24.	Gwarancja na sprzęt przynajmniej trzy lata, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.
25.	Produkt musi być fabrycznie nowy i dostarczony przez autoryzowany kanał sprzedaży producenta na terenie kraju.
26.	Szyny do montażu w szafie rack.
1.	Minimum 24 portów w standardzie 1000/10000BaseT
2.	Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP).
3.	Przepustowość: minimum 560 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)
4.	Wydajność: minimum 415 Mp/s
5.	Tablica adresów MAC o wielkości minimum 16000 pozycji
6.	Obsługa ramek Jumbo
7.	Wielkość sprzętowej tablicy routingu statycznego: minimum 64 wpisów dla IPv4, minimum 64 wpisów dla IPv6
8.	Obsługa routingu dla VLAN

9.	Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping
10.	Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol
11.	Obsługa IEEE 802.1Q oraz minimum 512 jednoczesnych sieci VLAN
12.	Wsparcie dla funkcji DHCP server, DHCP Relay oraz DHCP Snooping
13.	Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI
14.	Funkcja mirroringu portów
15.	Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)
16.	Funkcja autoryzacji użytkowników zgodna z 802.1x
17.	Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+
18.	RADIUS Accounting
19.	Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az
20.	Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, http i https
21.	Obsługa Syslog
22.	Obsługa NTP lub SNTP
23.	Wsparcie dla funkcji Private VLAN lub równoważnego
24.	Minimalny zakres pracy od 0°C do 45°C
25.	Wysokość w szafie 19" – 1U, głębokość nie większa niż 50 cm
26.	Minimum 3 wewnętrzne wentylatory
27.	Wewnętrzny zasilacz 230V
28.	Maksymalny pobór mocy nie większy niż 200W
29.	3 letnia gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.

II.1.7 Przełącznik dostępowy sieci LAN typ 1 bez PoE - 4 sztuki

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

WYMAGANE MINIMALNE PARAMETRY TECHNICZNE	
1.	Minimum 48 portów gigabitowych w standardzie 100/1000BaseT
2.	Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP).
3.	Przepustowość: minimum 176 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)
4.	Wydajność: minimum 112 Mp/s
5.	Tablica adresów MAC o wielkości minimum 32000 pozycji
6.	Obsługa ramek Jumbo
7.	Routing IPv4 – minimum: statyczny, RIPv2, OSPF (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów)
8.	Routing IPv6 – minimum: statyczny, RIPng, OSPFv3 (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów)
9.	Wielkość sprzętowej tablicy routingu: minimum 2000 wpisów dla IPv4, 1000 wpisów dla IPv6
10.	Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping
11.	Obsługa VxLAN
12.	Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol
13.	Obsługa 4094 tagów IEEE 802.1Q oraz minimum 2000 jednoczesnych sieci VLAN
14.	Funkcja Root Guard oraz BPDU protection
15.	Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 8 urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie

	dopuszcza się rozwiązań typu klaster). Jeżeli łączenie w stos wymaga dodatkowych modułów lub licencji to dostarczenie ich jest wymagane w ramach tego postępowania
16.	Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie
17.	Wsparcie dla funkcji DHCP server, DHCP Relay oraz DHCP Snooping
18.	Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI
19.	Obsługa standardu 802.1p – min. 8 kolejek na porcie
20.	Funkcja mirroringu portów
21.	Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)
22.	Funkcja autoryzacji użytkowników zgodna z 802.1x
23.	Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+
24.	RADIUS Accounting
25.	Wsparcie dla protokołu OpenFlow w wersji 1.0 oraz 1.3
26.	OpenFlow musi posiadać możliwość konfiguracji przetwarzania pakietów przez przełącznik w oparciu o ciąg tablic.
27.	Musi być możliwe wielotablicowe przetwarzanie zapytań OpenFlow zawierająca następujące tablice do przetwarzania reguł sprzętowo w oparciu o: źródłowe i docelowe adresy MAC, źródłowy i docelowy adres IP oraz nr portu, numer portu wejściowego (pole IP DSCP oraz VLAN PCP)
28.	Musi być możliwe przypisywanie więcej niż jednej akcji zadanemu wpisowi OpenFlow.
29.	Musi być możliwe tworzenie logicznych tuneli poprzez komunikaty SNMP i możliwość ich wykorzystania w kierowaniu ruchem w sposób sterowany za pomocą protokołu OpenFlow.
30.	Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az
31.	Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https
32.	Obsługa Syslog
33.	Obsługa NTP lub SNTPv4
34.	Musi być możliwość przechowywania co najmniej dwóch wersji oprogramowania na przełączniku
35.	Musi być możliwość przechowywania co najmniej trzech plików konfiguracyjnych na przełączniku, możliwość wgrywania i zgrzywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej
36.	Wsparcie dla funkcji Private VLAN lub równoważnego
37.	Obsługa protokołu VTP lub MVRP

38.	Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Uni-Directional Link Detection (UDLD) lub Device Link Detection Protocol (DLDP) lub równoważnego
39.	Minimalny zakres pracy od 0°C do 45°C
40.	Wysokość w szafie 19" – 1U, głębokość nie większa niż 50 cm
41.	Wewnętrzny zasilacz 230V
42.	Maksymalny pobór mocy nie większy niż 100W
43.	Przełącznik musi być w pełni wspierany przez system zarządzania opisany w punkcie II.1.10. W szczególności system zarządzania musi występować na oficjalnej liście sprzętu kompatybilnego z przełącznikiem.
44.	3 letnia gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Wymagane jest zapewnienie technicznego (niezależnego od zgłaszania usterek) wsparcia telefonicznego w trybie 8x5 przez okres co najmniej 3 lat. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis (przedstawiciela). Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.
45.	Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji

II.1.8 Przełącznik dostępowy sieci LAN typ 2 z obsługą PoE - 4 sztuki

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

WYMAGANE MINIMALNE PARAMETRY TECHNICZNE	
1.	Minimum 48 portów gigabitowych w standardzie 100/1000BaseT ze wsparciem dla standardu 802.3at (PoE+)
2.	Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP).

3.	Przepustowość: minimum 176 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)
4.	Wydajność: minimum 112 Mp/s
5.	Tablica adresów MAC o wielkości minimum 32000 pozycji
6.	Obsługa ramek Jumbo
7.	Routing IPv4 – minimum: statyczny, RIPv2, OSPF (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów)
8.	Routing IPv6 – minimum: statyczny, RIPv6, OSPFv3 (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów)
9.	Wielkość sprzętowej tablicy routingu: minimum 2000 wpisów dla IPv4, 1000 wpisów dla IPv6
10.	Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping
11.	Obsługa VxLAN
12.	Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol
13.	Obsługa 4094 tagów IEEE 802.1Q oraz minimum 2000 jednoczesnych sieci VLAN
14.	Funkcja Root Guard oraz BPDU protection
15.	Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 8 urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Jeżeli łączenie w stos wymaga dodatkowych modułów lub licencji to dostarczenie ich jest wymagane w ramach tego postępowania
16.	Automatyczne wykrywanie punktów bezprzewodowych podłączonych do przełącznika (automatyczne konfigurowanie portów, do których są one podłączone (minimum sieć VLAN, CoS, budżet mocy PoE, priorytet PoE)
17.	Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie
18.	Wsparcie dla funkcji DHCP server, DHCP Relay oraz DHCP Snooping
19.	Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI
20.	Obsługa standardu 802.1p – min. 8 kolejek na porcie

21.	Funkcja mirroringu portów
22.	Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)
23.	Funkcja autoryzacji użytkowników zgodna z 802.1x
24.	Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+
25.	RADIUS Accounting
26.	Wsparcie dla protokołu OpenFlow w wersji 1.0 oraz 1.3
27.	OpenFlow musi posiadać możliwość konfiguracji przetwarzania pakietów przez przełącznik w oparciu o ciąg tablic.
28.	Musi być możliwe wielotablicowe przetwarzanie zapytań OpenFlow zawierająca następujące tablice do przetwarzania reguł sprzętowo w oparciu o: źródłowe i docelowe adresy MAC, źródłowy i docelowy adres IP oraz nr portu, numer portu wejściowego (pole IP DSCP oraz VLAN PCP)
29.	Musi być możliwe przypisywanie więcej niż jednej akcji zadanemu wpisowi OpenFlow.
30.	Musi być możliwe tworzenie logicznych tuneli poprzez komunikaty SNMP i możliwość ich wykorzystania w kierowaniu ruchem w sposób sterowany za pomocą protokołu OpenFlow.
31.	Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az
32.	Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https
33.	Obsługa Syslog
34.	Obsługa NTP lub SNTPv4
35.	Musi być możliwość przechowywania co najmniej dwóch wersji oprogramowania na przełączniku
36.	Musi być możliwość przechowywania co najmniej trzech plików konfiguracyjnych na przełączniku, możliwość wgrywania i zgrzywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej
37.	Wsparcie dla funkcji Private VLAN lub równoważnego
38.	Obsługa protokołu VTP lub MVRP
39.	Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Uni-Directional Link Detection (UDLD) lub Device Link Detection Protocol (DLDP) lub równoważnego
40.	Minimalny zakres pracy od 0°C do 45°C
41.	Wysokość w szafie 19" – 1U, głębokość nie większa niż 50 cm
42.	Wewnętrzny zasilacz 230V zapewniający budżet mocy PoE na poziomie nie niższym niż 370W

43.	Maksymalny pobór mocy (bez PoE) nie większy niż 250W
44.	Przełącznik musi być w pełni wspierany przez system zarządzania opisany w punkcie II.1.10 W szczególności system zarządzania musi występować na oficjalnej liście sprzętu kompatybilnego z przełącznikiem.
45.	3 letnia gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Wymagane jest zapewnienie technicznego (niezależnego od zgłaszania usterek) wsparcia telefonicznego w trybie 8x5 przez okres co najmniej 3 lata. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis (przedstawiciela). Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.
46.	Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.

II.1.9 Kompletny Punkt sieci bezprzewodowej wraz z dedykowanym zestawem montażowym

Wymagane jest dostarczenie 15 szt. Punktów dostępowych spełniających poniżej opisane minimalne parametry funkcjonalne:

WYMAGANE MINIMALNE PARAMETRY TECHNICZNE	
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 wave 2/ax, oraz 2.4GHz b/g/n/ax.
2.	Punkt dostępowy musi mieć możliwość współpracy z centralnym kontrolerem sieci bezprzewodowej

3.	<p>Punkt dostępowy musi mieć możliwość pracy w trybie autonomicznym tj. bez nadzoru centralnego kontrolera:</p> <ul style="list-style-type: none"> a. Punkt dostępowy musi posiadać funkcjonalność zarządzania przez przeglądarkę internetową i protokół https b. Wszystkie operacje konfiguracyjne muszą być możliwe do przeprowadzenia z poziomu przeglądarki c. Przełączenie punktu dostępowego do pracy z centralnym kontrolerem może odbywać się tylko poprzez zmianę ustawienia trybu pracy urządzenia z poziomu GUI. Zmiana trybu pracy nie może się odbywać poprzez instalację na urządzeniu, nowej wersji oprogramowania.
4.	<p>Musi być zapewniona możliwość wspólnej konfiguracji punktów połączonych w jedną sieć LAN w warstwie 2:</p> <ul style="list-style-type: none"> a. System operacyjny zainstalowany w punktach dostępowych musi umożliwiać automatyczny wybór jednego punktu dostępowego jako elementu zarządzającego b. W przypadku awarii punktu zarządzającego kolejny punkt dostępowy w sieci musi przejąć jego rolę w sposób automatyczny c. Modyfikacja konfiguracji musi się automatycznie propagować na pozostałe punkty dostępowe d. Obraz systemu operacyjnego musi się automatycznie propagować na pozostałe punkty dostępowe, aby wszystkie punkty miały tą samą jego wersję e. Tworzenie klastra do 130 urządzeń
5.	<p>Punkt dostępowy musi mieć możliwość pracy w trybie monitorującym pasmo radiowe w celu wykrywania np. fałszywych AP</p>
6.	<p>W system operacyjny musi być wbudowana pełnostanowa zapora sieciowa</p>
7.	<p>W system musi być wbudowany serwer DHCP</p>

8.	W system musi być wbudowany serwer RADIUS umożliwiający terminowanie sesji EAP bezpośrednio na urządzeniach, bez pośrednictwa zewnętrznych elementów
9.	Musi być obsługiwane terminowanie sesji EAP w nie mniej niż następujących opcjach: <ul style="list-style-type: none"> a. EAP-TLS b. PEAP-MSCHAPv2 c. PEAP-GTC d. TTLS-MSCHAPv2
10.	Musi istnieć możliwość integracji z zewnętrznymi serwerami uwierzytelniania RADIUS oraz LDAP
11.	Punkt dostępowy musi obsługiwać nie mniej niż 16 niezależnych SSID
12.	Każde SSID musi mieć możliwość przypisania w sposób statyczny lub dynamiczny do sieci VLAN
13.	Musi istnieć możliwość uwierzytelniania użytkowników za pomocą portalu WWW, przynajmniej poprzez: <ul style="list-style-type: none"> a. Portal wbudowany w urządzenie, bez konieczności instalowania jakichkolwiek dodatkowych urządzeń/oprogramowania b. Zewnętrzny portal WWW
14.	Musi być zapewniona możliwość zdefiniowania odseparowanej sieci gościnnej z funkcją NAT
15.	Wbudowany serwer uwierzytelniający musi obsługiwać konta gościnne
16.	Zarządzanie pasmem radiowym w sieci punktów dostępowych musi się odbywać automatycznie za pomocą auto-adaptacyjnych mechanizmów, w tym nie mniej niż:

	<ul style="list-style-type: none"> a. Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe b. Stałe monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu c. Rozkład ruchu pomiędzy różnymi punktami dostępowym oraz pasmami bazując na ilości użytkowników oraz użyciu pasma d. Wykrywanie interferencji oraz miejsc bez pokrycia sygnału e. Automatyczne przekierowywanie klientów, którzy mogą pracować w pasmie 5GHz f. Wyrównywanie czasów dostępu do pasma dla klientów pracujących w standardzie 802.11n/ac wave 2 oraz starszych (802.11b/g) g. Wsparcie dla 802.11d oraz 802.11h h. Możliwość stworzenia profili czasowych w których dane SSID ma być rozgłaszane
17.	Minimalizacja interferencji związanych z sieciami 3G/4G LTE
18.	Punkt dostępowy musi mieć wbudowany moduł Bluetooth Low Energy (BLE5.0) (co najmniej 7dBm) wykorzystywany w systemie nawigacji wewnątrzbudynkowej
19.	Punkt dostępowy musi mieć wbudowany moduł Zigbee (802.15.4) (co najmniej 7dBm)
20.	Obsługa roamingu klientów w warstwie 2
21.	Obsługa monitoringu przez SNMP
22.	Obsługa logowania na zewnętrznym serwerze SYSLOG
23.	W system musi być wbudowany mechanizm wykrywania ataków na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci
24.	W system musi być wbudowany mechanizm zapobiegania atakom na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci

25.	<p>Wbudowany interfejs zarządzania musi dostarczać następujących informacji o systemie:</p> <ol style="list-style-type: none"> Widok diagnostyczny prezentujący problemy z sygnałem/prędkością Wykorzystanie pasma Ilość klientów korzystających z systemu/interferujących Ilość ramek wejściowych/wyjściowych dla każdego radia Ilość odrzuconych/błędnych ramek/s dla każdego radia Szum tła dla każdego radia Wyświetlanie logów systemowych
26.	<p>Punkt dostępowy musi posiadać 4 wbudowane anteny pracujące w trybie 4x4 MIMO, z parametrami co najmniej: 4 dBi dla 2,4GHz, 7.5 dBi dla 5 GHz</p>
27.	<p>Obsługa standardów 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac 1 Wave, 802.11ac 2 Wave, 802.11ax</p>
28.	<p>Praca w trybie SU MIMO 4X4:4 dla 5GHz</p>
29.	<p>Specyfikacja radia 802.11a/n/ac/ax:</p> <ol style="list-style-type: none"> Obsługiwana technologia OFDM oraz OFDMA Typy modulacji: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM Moc transmisji konfigurowalna przez administratora – możliwość zmiany co 0.5dbm Prędkości transmisji: <ul style="list-style-type: none"> 6, 9, 12, 18, 24, 36, 48, 54 Mbps dla 802.11a, MCS0-MCS23 (6,5Mbps do 450Mbps) dla 802.11n MCS0-MCS9, NSS = 1-4 (6.5 Mbps do 1733 Mbps) dla 802.11ac MCS0 do MCS11, NSS = 1-2 (3.6 Mbps do 574 Mbps) dla 802.11ax (2,4GHz) MCS0 do MCS11, NSS = 1-4 (3.6 Mbps do 4803 Mbps) dla 802.11ax (5GHz) Obsługa HT – kanały 20/40MHz dla 802.11n Obsługa VHT – kanały 20/40/80/160MHz dla 802.11ac

	<p>g. Obsługa HE – kanały 20/40/80/160MHz dla 802.11ax</p> <p>h. Wsparcie dla technologii DFS (Dynamic frequency selection) – dla wszystkich 80Mhz kanałów w paśmie 5GHz</p> <p>i. Agregacja pakietów: A-MPDU, A-MSDU dla standardów 802.11n/ac</p> <p>j. Wsparcie dla:</p> <ul style="list-style-type: none"> • MRC (Maximal ratio combining) • CDD/CSD (Cyclic delay/shift diversity) • STBC (Space-time block coding) • LDPC (Low-density parity check) • Technologia TxBF
30.	<p>Specyfikacja radia 802.11b/g/n/ax:</p> <p>a. Częstotliwość 2,400 ~2,4835</p> <p>b. Technologia direct sequence spread spectrum (DSSS), OFDM, OFDMA</p> <p>c. Typy modulacji – CCK, BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM</p> <p>d. Moc transmisji konfigurowalna przez administratora</p>
31.	<p>Punkt dostępowy musi posiadać co najmniej:</p> <p>a. 1 interfejs 100/1000 BaseT</p> <ul style="list-style-type: none"> • z funkcją auto-sensing link oraz MDI/MDX • obsługa równoważenie obciążenia „load balancing” <p>b. 1 interfejs 100/1000/2.5G BaseT (zgodny z 802.3bz)</p> <ul style="list-style-type: none"> • z funkcją auto-sensing link oraz MDI/MDX • z funkcją PoE/PoE+ • obsługa równoważenie obciążenia „load balancing” <p>c. interfejs konsoli RS-232 (RJ-45) lub USB</p> <p>d. interfejs USB 2.0 (Typ-A, niezależny od portu konsoli)</p> <p>e. przycisk przywracający konfigurację fabryczną</p> <p>f. slot zabezpieczający Kensington lub równoważny</p>
32.	<p>Parametry pracy urządzenia:</p> <p>a. Temperatura otoczenia (zakres minimalny): 0-50 ° C</p> <p>b. Wilgotność (zakres minimalny): 5% - 92%</p> <p>c. Obsługiwane standardy:</p>

	<ul style="list-style-type: none"> • Ethernet IEEE 802.3 / IEEE 802.3u • Power-over-Ethernet IEEE 802.3af • Wireless IEEE 802.11a/b/g/n/ac/ax <ul style="list-style-type: none"> d. Znak CE e. EN 300 328 f. EN 301 489 g. EN 301 893 h. EN 60601-1-1, EN60601-1-2
33.	Punkt dostępowy zasilony przy użyciu zgodnym ze standardem 802.3at PoE.
34.	Urządzenie musi posiadać certyfikat Wi-Fi Alliance (WFA) dla standardów 802.11/a/b/g/n/ac
35.	Wszystkie dostępne na urządzeniu funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.
36.	Punkt dostępowy musi zostać dostarczony z elementami montażowymi niezbędnymi do montażu na płaskiej powierzchni
37.	Punkt dostępowy musi być objęty co najmniej gwarancją producenta tj. gwarancją przez 3 lata. Gwarancja realizowana jest przez zwrot zepsutego urządzenia do producenta, który w terminie nie dłuższym niż 10 dni przesyła zamiennik. Gwarancja musi być realizowana bezpośrednio przez producenta sprzętu lub autoryzowany kanał serwisowy (przedstawiciela).

II.1.10 Oprogramowanie do zarządzania siecią – licencje na 30 urządzeń

Zamawiający oczekuje dostarczenia licencji oprogramowania do zarządzania siecią co najmniej 30 urządzeń spełniających poniższe parametry minimalne:

WYMAGANE MINIMALNE PARAMETRY TECHNICZNE	
1.	Dedykowane oprogramowanie służące do zarządzania i monitorowania pracy wszystkimi urządzeniami opisanymi w punktach 2,3,4. Oprogramowanie musi być wyposażone w licencję pozwalającą na zarządzaniem minimum 30 urządzeniami sieciowymi każdego typu (licencja

	nie może być ograniczona do jednego typu urządzeń, jeżeli dany typ urządzeń wymaga oddzielnego licencjonowania, muszą być one zaoferowane ponad wymagane minimum).
2.	System Zarządzania i Monitoringu tego samego producenta co urządzenia zainstalowane w sieci WLAN i LAN
3.	Oprogramowanie umożliwiające instalacje w środowisku wirtualnym VMware
4.	Obsługa poprzez interfejs graficzny z wykorzystaniem przeglądarki WWW
5.	Zarządzanie wszystkimi punktami dostępowymi AP oraz kontrolerami Sieci Radiowej będących przedmiotem tego samego postępowania
6.	System musi posiadać odpowiednią ilość licencji do obsługi wszystkich niezbędnych urządzeń.
7.	Wsparcie środowisk heterogenicznych, czyli możliwość zarządzania z wykorzystaniem SNMP urządzeniami sieciowymi różnych producentów
8.	Automatyczne wykrywanie urządzeń
9.	Bieżące monitorowanie stanu wszystkich podłączonych urządzeń
10.	Funkcja automatycznej konfiguracji urządzeń sieci radiowej po podłączeniu się ich do sieci
11.	Funkcja zbierania i wyświetlania informacji dotyczących pracujących w sieci urządzeń klienckich oraz możliwość ich wyszukania przy użyciu różnych parametrów takich jak: <ul style="list-style-type: none"> a. system operacyjny b. typ urządzenia c. użytkowanego urządzenia sieci WLAN oraz danego SSID
12.	Funkcja pełnej wizualizacji położenia urządzeń znajdujących się w sieci
13.	Funkcja archiwizacji konfiguracji urządzeń
14.	Konfiguracja zadań dla podłączonych urządzeń, w szczególności <ul style="list-style-type: none"> a. automatyczna zmiana wersji oprogramowania urządzeń, b. ponowne uruchomienie urządzenia c. definiowanie przedziałów czasowych, w których dane SSID ma być rozgłaszane

15.	Narzędzie ułatwiające planowanie radiowe dla sieci posiadające możliwość wizualizacji pokrycia radiowego
16.	Funkcja tworzenia map pokrycia (tzw. Heat Map)
17.	Panel zarządzający GUI umożliwiający wyświetlanie przynajmniej <ul style="list-style-type: none"> a. Wykresu liczby zasocjowanych urządzeń klienckich b. Wykresu potencjalnej przepustowości urządzeń klienckich c. Wykresu stosunku sygnał do szumu (SNR) urządzeń klienckich
18.	Funkcja automatycznego wykrycia urządzeń fałszywych, jego lokalizacji oraz ich ograniczenie np. poprzez rozłączenie urządzeń podłączonych do AP
19.	Funkcja generowania ostrzeżeń i logów dotyczących wykrytych ataków w sieci bezprzewodowej
20.	Funkcja generowania wiadomości email dla administratorów sieci (alerty, ostrzeżenia)
21.	Funkcja definiowania poziomu dostępu dla administratorów z przypisanymi: <ul style="list-style-type: none"> a. Rolami b. Segmentami sieci, do których uzyskuje się dostęp
22.	Obsługa XMP API
23.	Funkcja monitorowania jakości oraz ilości połączeń Unified Communication and Collaboration
24.	Minimum 12 miesięczna gwarancja producenta. Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 24x7 na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis (przedstawiciela). Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.
25.	Wszystkie dostarczone licencje i obsługiwane funkcje muszą być permanentne, nie dopuszcza się licencji czasowych

II.1.11 Oprogramowanie do wirtualizacji – 1 komplet

WYMAGANE MINIMALNE PARAMETRY TECHNICZNE	
<p>Wykonawca zobowiązany jest do dostarczenia kompletu licencji oprogramowania do wirtualizacji na dostarczanych serwerach, obejmujących łącznie 2 procesory fizyczne.</p> <p>Licencje powinny być dostarczone wraz z 5 letnim wsparciem, świadczonym przez producenta będącego licencjodawcą oprogramowania. Pierwsza linia wsparcia świadczona przez producenta oprogramowania. Usługa wsparcia gwarancyjnego musi umożliwiać zgłaszanie problemów w dni robocze przez min 9 godzin z zakresu 8:00 – 17:00.</p>	
<p>Wymagania techniczne dot. oprogramowania</p>	<p>Warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 200MB pamięci operacyjnej RAM serwera fizycznego</p> <p>Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi potrafić obsłużyć i wykorzystać procesory fizyczne wyposażone w 576 logicznych wątków oraz do 12TB pamięci fizycznej RAM</p> <p>Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych</p> <p>Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 6 TB pamięci operacyjnej RAM</p> <p>Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych</p> <p>Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowo, 3 porty równoległe i 20 urządzeń USB</p> <p>Rozwiązanie musi wspierać następujące systemy operacyjne: MS-DOS 6.22, Windows XP, Windows Vista, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows 7, Windows 8, SLES 12, SLES 11, SLES 10, SLES 9, SLES 8, REHL 7, RHEL 6, RHEL 5, RHEL 4, RHEL 3, REHL Atomic 7, Solaris 11 ,Solaris 10, Solaris 9, Solaris 8, OS/2 Warp 4.0, Debian, CentOS, FreeBSD, Asianux, Mandriva, Ubuntu, SCO</p>

	<p>OpenServer, SCO Unixware, Mac OS X, Photon OS, eCommStation 1/2/2.1, Oracle Linux , CoreOS, NeoKylin</p> <p>Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji</p> <p>Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na zasobach dyskowych</p> <p>Rozwiązanie musi zapewniać sprzętowe wsparcie dla wirtualizacji zagnieżdżonej, w szczególności w zakresie możliwości zastosowania trybu XP mode w Windows 7 a także instalacji wszystkich funkcjonalności w tym Hyper-V pakietu Windows Server 2012 na maszynie wirtualnej</p> <p>Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji</p> <p>Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta root</p> <p>Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi</p> <p>Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością wskazania konieczności zachowania stanu pamięci pracującej maszyny wirtualnej.</p> <p>Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności: Microsoft Active Directory, Open LDAP</p>
--	--

	<p>Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej</p> <p>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. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów</p> <p>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</p> <p>Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN)</p> <p>Rozwiązanie musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi</p> <p>Rozwiązanie musi umożliwiać wykorzystanie technologii 10GbE w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi</p> <p>Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek</p> <p>Rozwiązanie musi zapewnić możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych</p> <p>Rozwiązanie musi zapewniać możliwość replikacji maszyn wirtualnych z dowolnej pamięci masowej w tym z dysków wewnętrznych serwerów fizycznych na dowolną pamięć masową w tym samym lub oddalonym ośrodku przetwarzania</p> <p>Rozwiązanie replikujące musi gwarantować współczynnik RPO na poziomie minimum 5 minut</p>
--	---

	<p>Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum. Konieczna jest możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi bez przerywania pracy usług</p> <p>Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi oraz różnymi konsolami do zarządzania wirtualizacją. Rozwiązanie musi posiadać natywne mechanizmy szyfrowania, podczas przenoszenia maszyn wirtualnych, w czasie ich pracy pomiędzy serwerami fizycznymi</p> <p>Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały automatycznie przełączone na inne serwery infrastruktury</p> <p>Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury bez utraty danych</p> <p>Rozwiązanie musi zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania</p> <p>Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej wliczając w to zarówno poprawki bezpieczeństwa jak i zmianę jej wersji bez potrzeby wyłączania wirtualnych maszyn</p> <p>Rozwiązanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci</p> <p>Decyzja o próbie przywrócenia funkcjonalności maszyny wirtualnej w przypadku awarii lub niedostępności serwera fizycznego powinna być podejmowana automatycznie, jednak musi istnieć możliwość określenia przez administratora czasu po jakim taka decyzja jest wykonywana</p>
--	--

Rozwiązanie musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (o maksymalnie dwóch procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii serwerów fizycznych, bez utraty danych i dostępności danych podczas awarii serwerów fizycznych

Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek

Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB

Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej

Rozwiązanie musi umożliwiać konfigurację HA dla każdego swojego komponentu w celu unikania awarii pojedynczego elementu

System musi wspierać mechanizmy zaawansowanego uwierzytelniania do systemu operacyjnego wirtualnej maszyny za pomocą technologii Smart Card Reader

Wirtualizator musi wspierać TPM 2.0 oznacza to min. że TPM zapewnia mechanizm gwarantujący, że serwer fizyczny uruchomił się z włączoną opcją Secure Boot. Po potwierdzeniu, że Secure Boot jest włączone, system gwarantuje, że wirtualizator uruchomił w prawidłowej, niezmienionej formie poprzez weryfikację podpisu cyfrowego

Wirtualizator musi mieć włączenia funkcji “Microsoft virtualization-based security”, tzw. Microsoft VBS dla systemów operacyjnych maszyn wirtualnych opatrych o system operacyjny Windows 10 oraz Windows Server 2016.

System musi posiadać certyfikację FIPS-140-2 min. dla modułu jądra wirtualizatora odpowiedzialnego za szyfrowanie danych

Wirtualizator musi posiadać funkcjonalność wirtualnego TPM 2.0 dla maszyn wirtualnych Windows 10 oraz Windows 2016. Oznacza to, że punktu widzenia maszyny wirtualnej z systemem operacyjnym Windows 10 lub Windows 2016 wirtualny TPM widziany jest jako standardowy TPM, gdzie można przechowywać

	<p>bezpiecznie wrażliwe dane np. certyfikaty. Zawartość wirtualnego TPM przechowywana jest w pliku przynależnym do maszyny wirtualnej oraz musi być szyfrowana. W związku z tym wszystkie standardowe funkcjonalności wirtualizatora tj. wysoka dostępność, czy przenoszenie maszyn wirtualnych bez ich wyłączania pomiędzy różnymi serwerami fizycznymi działa prawidłowo. Wirtualizator musi posiadać rolę administratora odpowiedzialnego za zarządzanie kluczami szyfrującymi. Rola ta powinna być odseparowana od roli administratora wirtualizatora. Oznacza, to, że tylko administrator odpowiedzialny za szyfrowanie ma dostęp do kluczy szyfrujących oraz może zarządzać procesem szyfrowania w obrębie wirtualizatora</p> <p>Wirtualizator musi posiadać funkcjonalność szybkiego uruchamiania wirtualizatora po przeprowadzonym procesie jego aktualizacji. Taka funkcjonalność powoduje, że w procesie aktualizacji wirtualizatora, jeśli wymagany jest jego restart, eliminowana jest czasochłonna faza inicjalizacji serwera fizycznego – następuje skrócenia czasu wymaganego do ponownego uruchomienia serwera fizycznego podczas operacji aktualizacji</p> <p>Dostarczone oprogramowanie musi zapewniać możliwość wirtualizacji dla wszystkich dostarczonych w ramach postępowania serwerów</p> <p>Rozwiązanie musi posiadać wsparcie dla natywnych dysków 4K</p> <p>Rozwiązanie musi posiadać mechanizm, który ogranicza dostęp do indywidualnego zarządzania warstwą wirtualizacji na serwerach fizycznych w ramach klastra serwerów w celu utwardzenia/hardening (maksymalnego zwiększenia bezpieczeństwa dostępu) systemu wirtualizacji. System musi umożliwiać zarządzanie całą warstwą wirtualizacji z jednego bezpiecznego systemu do zarządzania z kontrolą dostępu.</p>
<p>Wymagania ogólne</p>	<p>Dostarczona licencja na oprogramowanie spełniające powyższe wymagania musi posiadać możliwość swobodnego przeniesienia na dowolny podmiot wymieniony w umowie ramowej i dowolny serwer fizyczny będący w posiadaniu Zamawiającego (bez ograniczeń licencji OEM). Licencje dostępne w modelu licencjonowania na procesor fizyczny (nielimitowana ilość rdzeni procesora).</p>

II.1.12 Oprogramowanie do backupu – 1 komplet

WYMAGANE MINIMALNE PARAMETRY TECHNICZNE	
<p>Wykonawca dostarczy licencje na oprogramowanie do backupu obejmujące dostarczane Serwer Aplikacyjne oraz serwer bazodanowy wraz z dostępem do aktualizacji przez okres 36 miesięcy.</p> <p>W przypadku zaoferowania większej ilości serwerów przez Wykonawcę, należy objąć wszystkie nowe serwery oprogramowaniem backupowym.</p>	
Funkcjonalność	<ul style="list-style-type: none"> • Oprogramowanie ma obsługiwać urządzenia taśmowe i dyskowe, służące do przechowywania kopii zapasowych danych. • Oprogramowanie musi posiadać graficzny interfejs zarządzania. • Oprogramowanie ma umożliwiać definiowanie w sposób centralny z jednej konsoli procesów polityki tworzenia kopii zapasowych, tj. określenia, jakie dane, kiedy i gdzie powinny być składowane (definiowanie, planowanie i zarządzanie harmonogramu backupu). • Oprogramowanie ma umożliwiać realizowanie raz zdefiniowanej polityki backupu w sposób automatyczny. • Oprogramowanie ma umożliwiać tworzenie kopii zapasowych całego wirtualnego środowiska • Oprogramowanie ma posiadać moduł monitorowania i raportowania systemu backupu. • Oprogramowanie ma umożliwiać na definiowanie kryteriów alarmów systemu backupu.
Kopie zapasowe	<ul style="list-style-type: none"> • Oprogramowanie musi zapewnić kompleksową ochronę maszyn wirtualnych dla maszyn wirtualnych VMware i Hyper-V • Oprogramowanie musi wykorzystywać mechanizmy integracji Microsoft® Volume Shadow Copy Service lub VMware vStorage™ APIs for Data Protection
Odtwarzanie	<ul style="list-style-type: none"> • Odtworzenie może odbywać się na poziomie obrazu maszyny wirtualnej. • Odtworzenie całej maszyny. • Odtwarzanie baz danych Oracle, Microsoft SQL. • Odtwarzanie kontrolerów domeny Microsoft Active Directory.

Licencjonowanie	Oprogramowanie ma umożliwiać wyłącznie chronienie środowiska wirtualnego – brak limitów na chronioną ilość danych i ilość maszyn wirtualnych.
------------------------	---

II.1.13 Baza danych – 2 szt.

LP.	WYMAGANIE MINIMALNE
1	Baza danych na dedykowanej platformie witalizacyjnej z przydzieloną odpowiednią ilością licencji dla 1 CPU wraz z asystą techniczną. Zamawiający dopuszcza wykorzystanie licencji ASFU (application specific), której ograniczeniem tego typu licencji jest przypisanie do konkretnej aplikacji.
2	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 Linux 32-bit i 64-bit, MS Windows 32-bit i 64-bit (lub równoważne). Oprogramowanie nie może mieć limitów na ilość przechowywanych danych – zarówno tekstowych, jak i multimedialnych.
3	Przetwarzanie transakcyjne wg reguł ACID (Atomicity, Consistency, Independency, Durability) z zachowaniem spójności i maksymalnego możliwego stopnia współbieżności.
4	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 zagnieżdżenia 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	Możliwość utworzenia wielu aktywnych zbiorów rezultatów (zapytań, instrukcji DML) w jednej sesji bazy danych.
10	Wsparcie protokołu XA.
11	Wsparcie standardu JDBC 3.0.

12	Zgodność ze standardem ANSI/ISO SQL 2003 lub nowszym w tym PL/SQL (Oracle), PL/pgSQL (PostgreSQL) czy T-SQL (Microsoft).
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 limit wielkości bazy do 524PB.
15	Wsparcie dla procedur i funkcji składowanych w bazie danych. Język programowania powinien być językiem proceduralnym, blokowym oraz wspierającym obsługę wyjątków. W przypadku, gdy wyjątek nie ma zadeklarowanej obsługi wewnątrz bloku, w razie jego wystąpienia wyjątek powinien być automatycznie propagowany do bloku nadrzędnego bądź wywołującej go jednostki programu. Procedury i funkcje składowane powinny mieć możliwość parametryzowania za pomocą parametrów prostych, jak i parametrów o typach złożonych, definiowanych przez użytkownika. Funkcje powinny mieć możliwość zwracania rezultatów jako zbioru danych, możliwego do wykorzystania jako źródło danych w instrukcjach SQL (czyli występujących we frazie FROM). Ww. jednostki programowe powinny umożliwiać wywoływanie instrukcji SQL (zapytania, instrukcje DML, DDL), umożliwiać jednoczesne otwarcie wielu tzw. kursorów pobierających paczki danych (wiele wierszy za jednym pobraniem) oraz wspierać mechanizmy transakcyjne (np. zatwierdzanie bądź wycofanie transakcji wewnątrz procedury).
16	Możliwość kompilacji procedur składowanych w bazie do postaci kodu binarnego (biblioteki dzielonej).
17	Możliwość deklarowania wyzwalaczy (triggerów) na poziomie instrukcji DML (INSERT, UPDATE, DELETE) wykonywanej na tabeli oraz na poziomie zdarzeń bazy danych (np. próba wykonania instrukcji DDL, start serwera, stop serwera, próba zalogowania użytkownika, wystąpienie specyficznego błędu w serwerze). Ponadto mechanizm wyzwalaczy powinien umożliwiać oprogramowanie obsługi instrukcji DML (INSERT, UPDATE, DELETE) wykonywanych na tzw. niemodyfikowalnych widokach (views). W przypadku, gdy w wyzwalaczu na poziomie instrukcji DML wystąpi błąd zgłoszony przez motor bazy danych bądź ustawiony wyjątek w kodzie wyzwalacza, wykonywana instrukcja DML musi być automatycznie wycofana przez serwer bazy danych, zaś stan transakcji po wycofaniu musi odzwierciedlać chwilę przed rozpoczęciem instrukcji, w której wystąpił ww. błąd lub wyjątek.
18	Możliwość autoryzowania użytkowników bazy danych za pomocą rejestru użytkowników założonego w bazie danych bądź mechanizmu wewnętrznego w stosunku do bazy danych.

19	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.
20	Przywileje użytkowników bazy danych powinny być określone 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.
21	Możliwość wykonywania i katalogowania kopii bezpieczeństwa bezpośrednio przez serwer bazy danych. Możliwość zautomatyzowanego usuwania zbędnych kopii bezpieczeństwa przy zachowaniu odpowiedniej liczby kopii nadmiarowych - stosownie do założonej polityki nadmiarowości backup'ów. Możliwość integracji z powszechnie stosowanymi systemami backupu (Legato, Veritas, Tivoli, OmniBack, ArcServe itd). Wykonywanie kopii bezpieczeństwa powinno być możliwe w trybie offline oraz w trybie online.
22	Możliwość wykonywania kopii bezpieczeństwa w trybie on-line (hot backup).
23	Baza danych będzie wykorzystana m.in. dla systemu HIS i ERP może być dla niego dedykowana. Zamawiający nie przewiduje wykorzystanie bazy danych do innych celów. Baza danych musi być licencjonowana na rdzenie procesora (wymagane dostarczenie licencji niezbędnej na pokrycie dostarczonych serwerów bazodanowych w pkt II.2.1.2). Zamawiający dopuszcza licencjonowania bazy danych w tzw. modelu runtime, asfu. Dopuszczalne jest zastosowanie dwóch oddzielnych instancji bazy danych ale na bazie tego samego producenta. Wykonawca składając ofertę winien złożyć również oświadczenie zawierające informacje o wersji bazy danych wraz z podaniem jej producenta.
24	Baza danych musi zapewnić wysoką dostępność za pośrednictwem własnych mechanizmów lub dedykowanych komponentów zewnętrznych, które realizują następujące funkcjonalności: Oprogramowanie które jest łatwym w obsłudze narzędziem, służącym do zarządzania pamięciami masowymi bez konieczności przerywania ich pracy. Powinien umożliwić analizę wykorzystania dysków, grupowanie ich w wolumeny logiczne w celu lepszego wykorzystania i poprawy wydajności macierzy, stosowanie technik RAID oraz pomaga w wirtualizacji zasobów, a wszystko to bez potrzeby przerywania pracy systemów, zapewniając stałą dostępność i ochronę danych. Razem z oprogramowaniem musi zostać dostarczony wspierany przez producenta klastra system operacyjny. W celu uniknięcia SPoF rozwiązanie musi zapewniać wsparcie dla przełączania pomiędzy różnymi podsieciami w klastrze, należy odseparować konfigurację VLAN w szczególności w konfiguracjach klastrów geograficznych i kampusowych. Funkcjonalność ta jest niezbędna w rozwiązaniach DR;

Rozwiązanie powinno umożliwiać wsparcie do konfiguracji wieloklastrowej, tworzenie grup aplikacyjnych które mogą przełączać się pomiędzy różnymi klastrami.

Rozwiązanie musi zapewniać wsparcie dla klastrów kampusowych, wsparcie dla rozwiązań klastrów rozciągniętych pomiędzy dwoma ośrodkami. Wymagają one aby przynajmniej jeden aktualny obraz (mirror) danych produkcyjnych był dostępny w każdym ośrodku;

Rozwiązanie musi zapewniać wsparcie dla asymetrycznych serwerów, możliwość tworzenia rozwiązań klastrowych przy zastosowaniu serwerów o różnej konfiguracji (ilość procesorów, RAM, kart HBA, SAS);

Rozwiązanie musi posiadać Centralną Konsolę zarządzającą wieloma klastrami;

Rozwiązanie musi zapewniać możliwość wykorzystania funkcjonalności rozwiązania do budowy systemów DR (Disaster Recovery);

W celu zapewnienia optymalnej wydajności działania logika przełączania musi uwzględniać zależności pomiędzy serwisami, całkowitym i dostępnym potencjałem każdego z węzłów oraz także ich logicznym grupowaniem. Rozwiązanie musi zapewniać zaawansowaną logikę przełączania:

- a. przełączanie w obrębie zdefiniowanej strefy
- b. przełączanie w oparciu o bieżące obciążenie węzłów klastra
- c. logika uwzględniająca kontekst innych grup serwisowych
 - nigdy nie tym samym serwerze co ...
 - zawsze na tym samym serwerze co ...
 - zalecane na tym samym serwerze co ...
 - wyłącznie na tym samym serwerze co....

Rozwiązanie klastrowe musi zapewniać automatyczny wzrost wielkości wolumenów wraz z powiadamianiem administratora o wystąpieniu takiej zmiany.

Rozwiązanie klastrowe musi zapewniać automatyczny monitoring stanu systemu, informujący o aktualnym stanie systemu, a w szczególności informacje o przekroczeniu przyjętych wartości ułatwia proaktywne działanie podnoszące bezpieczeństwo rozwiązania.

Rozwiązanie musi zapewniać możliwość zmniejszania systemu plików bez konieczności rekreowania woluminu oraz systemu plików;

Rozwiązanie musi zapewniać wsparcie dla woluminów dynamicznych w klastrze umożliwiające migrację w trybie online pomiędzy macierzami;

Rozwiązanie powinno mieć możliwość wsparcia dla różnych mechanizmów replikacji umożliwiające wykorzystanie posiadanych już zasobów do rozbudowy do rozwiązań Disaster Recovery, a w szczególności zapewniać wsparcie dla wielowęzłowych klastrów geograficznych używających następujących technologii replikacji:

- a. EMC SRDF (A/S)
- b. EMC MirrorView

- c. HDS TrueCopy
- d. HP Continues Access
- e. NetApp SnapMirror
- f. IBM metroMirror
- g. Symantec VVR
- h. Oracle DataGuard
- i. IBM DB2 HA/DR

W celu zapewnienia standaryzacji i spójności rozwiązanie klastrowe powinno mieć możliwość wsparcia dla wielu platform sprzętowych i OS:

- a. AIX
- b. Linux
- c. HP-UX
- d. Solaris
- e. Windows 2008/2012

Rozwiązanie musi zapewniać przejrzyste dla aplikacji biznesowych testy możliwości failoveru do ośrodka zapasowego, funkcjonalność umożliwiającą testowanie poprawności działania planów DR bez wpływu na dostępność aplikacji i możliwość przełączenia do ośrodka zapasowego jest niezbędna dla większości krytycznych aplikacji;

Rozwiązanie musi zapewniać brak konieczności stosowania dysku quorum bez utraty funkcjonalności;

Rozwiązanie musi wykorzystywać rozszerzenie standardu SCSI-3 – Permanent Reservation gwarantującym integralność danych;

Rozwiązanie musi umożliwiać zatrzymanie serwisów klastra bez zatrzymywania procesów biznesowych;

Rozwiązanie musi zapewniać granularne uprawnienia dla grup serwisowych, w przypadkach gdy Administrator Systemu w ramach prowadzonych prac zostanie zmuszony do zatrzymania całości lub części usług. Klaster nie powinien przełączyć się na inny węzeł w klastrze i administrator powinien mieć prawa do grup serwisowych obsługujących technologię, którą on zarządza;

Rozwiązanie musi zapewniać wsparcie dla rozwiązań usuwających dane w sposób bezpieczny z fizycznych nośników dyskowych zapewniające, iż nośniki po takiej operacji nie będą umożliwiały odczytanie danych które przez ich wymazaniem się znajdowały na fizycznych nośnikach dyskowych;

Rozwiązanie musi zapewniać wsparcie dla procesu replikacji. Możliwość replikacji pomiędzy macierzami różnych typów, pochodzących od różnych producentów. Wsparcie replikacji synchronicznej, asynchronicznej i periodycznej. Wsparcie InBound Communication. Wsparcie replikacji poprzez firewall'e – NAT TCP/UDP.

Zarządzanie pasmem replikacji:

- Agregacja linków - Throttling – ograniczanie pasma

II.2 Wdrożenie oprogramowania Szpitalnego Systemu Informatycznego SSI i eUsług

II.2.1 Wymogi dotyczące interoperacyjności lub migracji dla oferowanego SSI

1. Wykonawca zobowiązuje się dostarczyć Zamawiającemu wymagane funkcjonalności oprogramowania SSI i eUsług w taki sposób, aby w jak najszerszym zakresie zostały zaspokojone potrzeby Zamawiającego. Zamawiający posiada wdrożony i działający Szpitalny System Informatyczny Clininet firmy CompuGroupMedical w zakresie modułów wskazanych w pkt. II.2.3 SOPZ zgodnych z listą funkcjonalności wskazanych w Załączniku nr. 1 do SOPZ. Zamawiający wymaga zachowania pełnej wzajemnej interoperacyjności z modułami/grupami/systemami funkcjonalności funkcjonującymi u Zamawiającego.
2. Szpitalny System Informatyczny, stanowiący źródło Elektronicznej Dokumentacji Medycznej EDM musi posiadać zaimplementowane i uruchomione mechanizmy integracji oraz zapewnić prawidłową integrację z systemem EDM,
3. Dla eUsług należy zapewnić spełnienie przez nie wymagań Web Content Accessibility Guidelines (WCAG 2.0), z uwzględnieniem poziomu AA, określonych w załączniku nr 4 do rozporządzenia.

II.2.2 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. 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 naprawcze (tzw. down time) odbywają się w godzinach od 5:00 do 7:00. W ciągu jednego miesiąca mogą odbyć się maksymalnie cztery takie przerwy. Czas planowych prac naprawczych (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.2.3 Wykaz posiadanych licencji

Lista modułów posiadanych przez Zamawiającego w instalacji KSO WUM:

HIS – CGM CLININET

MODUŁY*
Poradnia
Oddział
Izba przyjęć
Blok operacyjny
Administracja
Konfiguracja

*Zakres funkcjonalny poszczególnych modułów opisano w Załączniku nr 1 do SOPZ.

II.2.4 Oprogramowanie aplikacyjne – wymagania ogólne

1. Wykonawca zobowiązuje się dostarczyć Zamawiającemu określone funkcjonalności SSI i eUsług, poprzez dostawę nowego rozwiązania w taki sposób, aby w jak najszerszym zakresie zostały zaspokojone potrzeby Zamawiającego.
2. Zakres danych znajdujących się w HIS obejmujących dokumentowanie z procesu udzielania świadczeń składających się na dokumentację 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.
3. System powinien umożliwić wygenerowanie prawidłowych (zgodnych z opublikowanymi przez NFZ plikami walidującymi) komunikatów wymiany danych z NFZ dotyczących wszystkich umów na świadczenia w bieżącym roku rozliczeniowym i roku następnym, powinien umożliwić ciągłość rozliczeń z NFZ począwszy od dnia uruchomienia oprogramowaniao najmniej na środowisku produkcyjnym w tym również rozliczenie z NFZ dla pobytów otwartych na dzień uruchomienia SSI na środowisku produkcyjnym.
4. W Systemie muszą być zaimplementowane mechanizmy walidacji haseł zgodnie z wymaganiami ustawowymi przewidzianymi dla rodzaju danych przetwarzanych przez System.

5. System musi być dostosowany do struktury organizacyjnej Zamawiającego.
6. 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.
7. System musi mieć możliwość utrzymania co najmniej 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.
8. System musi mieć możliwość definiowania listy personelu białego (w szczególności lekarzy, pielęgniarek, położnych, techników) i ich specjalności zgodnie ze słownikiem i wymaganiami NFZ.
9. System musi być zintegrowany, przez co rozumie się zintegrowaną pracę wszystkich systemów/modułów w oparciu o swobodną, automatyczną wymienialność danych pomiędzy elementami (modułami) systemu.
10. System musi pozwalać na obsługę zdarzeń niepożądanych w określonym przedziale czasowym, nadawanie dostępu do funkcjonalności zgodnie z nadanymi uprawnieniami.
11. System musi posiadać możliwość zarejestrowania oraz analizy zdarzeń zgodnie ze standardami akredytacyjnymi publikowanymi przez Centrum Monitorowania Jakości w Ochronie Zdrowia.
12. 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.
13. Zamawiający zapewni współpracę z Producentami innych systemów Zamawiającego oraz SSI wskazanego w pkt II.2.3 przy uzyskaniu przez Wykonawcę opisów interfejsów do integracji, natomiast wykonanie integracji jest obowiązkiem Wykonawcy. Ustalenie kosztów integracji z systemami posiadanymi przez Zamawiającego jest obowiązkiem Wykonawcy. Zamawiający nie odpowiada za zawartość merytoryczną dokumentacji w zakresie opisów interfejsów, którą przekaże zainteresowanym stronom producent SSI.
14. Zamawiający dopuszcza integrację z obecnymi systemami dziedzicznymi tylko i wyłącznie poprzez wyspecyfikowane interfejsy, których implementację udostępnia dany system dziedziczny ze względu na to, że integracja bezpośrednia na poziomie bazy danych mogłaby doprowadzić do niekontrolowanej utraty integralności danych co w skrajnym przypadku grozi uszkodzeniem danych

wrażliwych procesu leczenia pacjentów.

15. Zamawiający nie przewiduje uczestnictwa w rozmowach z firmami trzecimi dotyczących integracji z ich systemami. Zamawiający wyjaśnia, że koszty integracji są częścią kosztu oferty składanej przez Wykonawcę w niniejszym postępowaniu.
16. Zamawiający wymaga spełnienia następujących warunków przez wdrożone oprogramowanie aplikacyjne:
 - a) zachowanie ciągłości obecnie stosowanych przez Zamawiającego oznaczeń dokumentacji medycznej,
 - b) umożliwienie kontynuacji sprawozdawania i rozliczania świadczeń udzielonych pacjentom przebywającym w szpitalu od kilkunastu lat (możliwość przesłania do NFZ pełnej historii hospitalizacji oraz historii rozliczeń), przy wykorzystaniu jednego modułu/oprogramowania,
 - c) umożliwienie dokonywania korekt zakwestionowanych przez NFZ świadczeń sprawozdanych i rozliczonych od roku 2010,
 - d) zachowanie przekazanej do NFZ historycznej numeracji zestawów świadczeń i procedur rozliczeniowych oraz zachowanie historycznej numeracji wszystkich innych danych przekazanych do NFZ i potwierdzonych, takich jak id uprawnień, numeracja sesji, numer przepustki, itp.,
 - e) zapewnienie możliwości wykonywania archiwalnych statystyk i raportów,
 - f) zapewnienie możliwości wykonywania kopii zapasowych struktur danych w trakcie ich pracy,
 - g) posiadanie sprawnego mechanizmu archiwizacji danych i mechanizmów gwarantujących spójność danych. Wymagane jest wzajemne współdziałanie modułów systemu medycznego i portalowego poprzez powiązania logiczne i korzystanie ze wspólnych danych przechowywanych na serwerach,
 - h) zapewnienie współpracy w zakresie eksportu danych z innym oprogramowaniem - pakietem oprogramowania biurowego (arkusz kalkulacyjny, edytor tekstów),
 - i) komunikaty systemowe i komunikacja z użytkownikiem w języku polskim,
 - j) możliwość korzystania z rozbudowanych odpowiedzi.
17. Zamawiający nie dysponuje dokumentacją techniczną systemów CLININET firmy CGM poza opisem interfejsu HL 7 stanowiącym Załącznik nr. 2 do SOPZ. Zamawiający nie dysponuje również kodami źródłowymi powyższego oprogramowania.
18. Uwzględniając powyższe, Wykonawca w ramach przedmiotu zamówienia zobowiązany będzie dokonać czynności zmierzających do analizy opisywanego wyżej oprogramowania w celu ustalenia i zidentyfikowania stosowanych w tym oprogramowaniu procedur odpowiedzialnych za wymianę danych oraz stanowiących interfejs wymiany danych (o ile w tym oprogramowaniu istnieją). Analiza

powinna określić jakiego rodzaju dane przekazywane są w ramach interfejsu wymiany danych, ustalić ich format, sposób zapisu i składowania w bazie danych. Jeżeli w wyniku przeprowadzonej analizy okaże się, iż oprogramowanie nie zawiera interfejsu wymiany danych lub dane udostępniane przez ten interfejs nie będą wystarczające dla zapewnienia funkcjonalności integracji w zakresie określonym w opisie przedmiotu zamówienia, Wykonawca dokona analizy funkcjonowania oprogramowania w zakresie umożliwiającym ustalenie sposobu zapisu, formatu danych i miejsca ich składowania w bazie danych (tabele, widoki, poszczególne pola w tablicach etc.). Czynności te mogą również obejmować badanie zawartych w oprogramowaniu algorytmów, jeżeli będzie to niezbędne dla właściwej interpretacji tych danych.

19. Do dokonania każdej z powyższych czynności z osobna lub ich wszystkich albo części czynności wyżej określonych Wykonawca uprawniony jest wyłącznie w jakim będą one niezbędne do osiągnięcia współdziałania dostarczanego w ramach niniejszego zamówienia z oprogramowaniem Zamawiającego.
20. Dla przeprowadzenia przedmiotowej analizy, Zamawiający przewiduje konieczność dokonania przez Wykonawcę czynności zwielokrotnienia kodu lub tłumaczenia jego formy w rozumieniu art. 74 ust. 4 pkt. 1 i 2 ustawy Prawo autorskie i prawa pokrewne w zakresie jaki niezbędny będzie do uzyskania informacji koniecznych do osiągnięcia współdziałania dostarczanego w ramach zamówienia oprogramowania z oprogramowaniem Zamawiającego. Dobór środków w zakresie tłumaczenia formy oprogramowania (np. dekompilacja oprogramowania) zapewniających osiągnięcie celu przedmiotowej analizy leży po stronie Wykonawcy. Czynności tłumaczenia formy oprogramowania, Wykonawca zobowiązany jest wykonać na własny koszt i ryzyko, w pełnym koniecznym zakresie z tym zastrzeżeniem, że:
 - a) czynności te będą odnosiły się tylko do tych części oprogramowania Zamawiającego, które będą niezbędne do osiągnięcia współdziałania tego oprogramowania z systemem dostarczanym przez Wykonawcę w ramach przedmiotowego zamówienia,
 - b) informacje uzyskane w ramach tych czynności nie będą:
 - wykorzystane do innych celów niż osiągnięcie współdziałania oprogramowania z oprogramowaniem dostarczanym przez Wykonawcę,
 - przekazane innym osobom, chyba że jest to niezbędne do osiągnięcia współdziałania niezależnie stworzonego programu komputerowego,
 - wykorzystane do rozwijania, wytwarzania lub wprowadzania do obrotu programu komputerowego o istotnie podobnej formie wyrażenia lub innych czynności naruszających prawa autorskie.
21. Informacje uzyskane przez Wykonawcę w toku wykonywania powyższych czynności stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy o zwalczaniu nieuczciwej konkurencji.

22. Wyniki przedmiotowej analizy stanowią podstawę do zapewnienia funkcjonalności integracji dostarczanego przez Wykonawcę w ramach zamówienia, systemu z funkcjonującym u Zamawiającego oprogramowaniem.
23. Zamawiający wymaga, by w przypadku wprowadzanych zmian przez producenta oprogramowania w systemie dziedzinowym Zamawiającego, Wykonawca w ramach integracji zapewnił wymianę danych pomiędzy systemem dziedzinowym SSI, a dostarczonym oprogramowaniem (aktualizacja wymiany danych musi nastąpić maksymalnie w ciągu 7 dni od dnia wprowadzenia zmiany w systemie dziedzinowym) przez okres 5 lat.
24. 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 eUsługi

Zamawiający wymaga w ramach przedmiotu zamówienia dostarczenia i wdrożenia eUsług współpracujących ze Szpitalnym Systemem Informatycznym co najmniej takich jak: Przetwarzanie EDM, e-Rejestracja, e-Zlecenia w zakresie nie mniejszym niż zostało to określone w dokumentach stanowiących Załącznik nr. 3 do SOPZ tj. Projekt wdrożenia e-Usług Referencyjnych (Przetwarzanie EDM, e-Rejestracja, e-Zlecenia).

Jednocześnie Zamawiający wymaga dostarczenia w ramach eUsług także możliwości:

- obsługi funkcjonalności udostępniania dokumentacji medycznej przez pacjenta tj. wyników badań, obrazów, itp. metodą zdalną. Wyniki badań udostępniane online pacjentom będą dotyczyć zarówno elementów dokumentacji jak i wyników obrazowych z systemu PACS, który będzie zintegrowany z systemem Zarządzania Elektroniczną Dokumentacją Medyczną.
- Obsługi funkcjonalności wywiadu medycznego - usługa umożliwi elektroniczne wprowadzenie przez pacjenta informacji dotyczących zdrowia jego i rodziny przed wizytą w celu skrócenia czasu wizyty. Usługa wywiadu jest szczególnie istotna w celu zebrania wszelkich niezbędnych informacji od pacjenta i wprowadzeniu ich do Elektronicznego Rekordu Medycznego. Dane wprowadzone na formularzach muszą być dostępne w systemie medycznym; ściśle zintegrowane z systemem informatycznym oraz formularzami

Dokumentacji Medycznej. Dzięki e-usłudze Pacjent będzie miał możliwość w dowolnym czasie, w dowolnym miejscu i za pomocą dowolnego urządzenia mobilnego mającego dostęp do sieci Internet, do uzupełniania informacji, celem przekazania ich do lekarza specjalisty. Rozwiązanie musi zdalnie prowadzić Pacjenta przez pytania pomocnicze, które będą pomocne w procesie wyboru sposobu leczenia. W odpowiedzi na umieszczony przez pacjenta opis, lekarz prowadzący może dopytać pacjenta o jego dolegliwości w odniesieniu do umieszczonego wpisu. Pacjent musi mieć możliwość dołączania zdjęć do swojego opisu.

II.4 **Dostawa i wdrożenie silnika bazy danych wraz z zasileniem danymi z obecnej posiadanej przez Zamawiającego bazy danych Adaptive Server Enterprise/15.5/EBF**

II.4.1 **Baza danych – wymagania ogólne**

Wykonawca wykona wszystkie prace programistyczne i migracyjne związane z zasileniem danymi w celu przeniesienia wszystkich funkcjonalności starego i 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 1 do niniejszego OPZ. 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 1 do OPZ - 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, bardziej wydajnej bazy danych, które umożliwi również przeniesienie na dostarczone w niniejszym postępowaniu macierz i serwery.

II.4.2 **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. Szczegółowy wykaz funkcji systemu, który użytkuje Zamawiający zawiera Załącznik nr 1 do SOPZ. Zamawiający w przypadku wątpliwości w tym zakresie może w toku badania ofert wezwać Wykonawcę do demonstracji systemu obejmującej wybrane cechy technologiczne spośród określonych w Wymaganiach Ogólnych dla poszczególnych podsystemów. Wykazanie braku realizacji cech technologicznych będzie podstawą do uznania, że treść oferty nie odpowiada treści specyfikacji istotnych warunków zamówienia.
2. **Oferent wraz z ofertą załączy** wykaz funkcji wraz z deklaracją działania tych funkcji na wydajnej platformie bazy danych.
3. 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.

4. System musi być uruchomiony i wdrożony we wszystkich komórkach organizacyjnych Zamawiającego.
5. 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.
6. 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.
7. Wykonawca jest zobowiązany do skonfigurowania procedur backupu systemu z wykorzystaniem narzędzi używanych przez Zamawiającego.

II.4.3 Interfejsy komunikacyjne

Zamawiający wymaga aby w zakresie nowo wdrażanych systemów objętym niniejszym zamówieniem, Wykonawca przedstawił stosowny dokument, opisujący „Interfejs komunikacyjny API systemu szpitalnego KSO 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.4.4 Opis stanu bieżącego

Zamawiający używa obecnie system klasy HIS (Hospital Information System) CliniNet, którego producentem jest CompuGroup Medical Polska sp. z o.o. (CGM) Zamawiający posiada następującą konfigurację systemu:

Licencje systemu CliniNet na użytkownika – 50 jednoczesnych użytkowników. **Zamawiający wymaga dostarczenia kolejnych licencji na użytkownika w zakresie posiadanych modułów uprawniających do pracy w systemie co najmniej 100 jednoczesnych użytkowników.**

Licencje na bazę danych Sybase – 4 licencje 15.5 (serwer bazodanowy 1, serwer raportowy).

Sybase Replication Serwer.

Serwery aplikacyjne i bazodanowe - 2

System CliniNet (obecna nazwa to CGM CLININET) zainstalowany i wdrożony jest na dwóch niezależnych instancjach bazy danych.

Informacje nt. bazy danych HIS

L.P.	ZAKRES DANYCH	ŚRODOWISKO BAZODANOWE	CZY ISTNIEJE MOŻLIWOŚĆ WYEKSPORTOWANIA WSKAZANEGO ZAKRESU DANYCH DO FORMATU ZEWNĘTRZNEGO? (TAK / NIE)	JEŚLI ISTNIEJE MOŻLIWOŚĆ WYEKSPORTOWANIA WSKAZANEGO ZAKRESU DANYCH, JAKI JEST TO FORMAT EKSPORTU?
1	dane o pacjentach i ich opiekunach,	Sybase	TAK	XML, CSV
2	Słownik personelu	Sybase	TAK	XML, CSV
3	Słownik jednostek kierujących,	Sybase	TAK	XML, CSV
4	Słownik lekarzy kierujących	Sybase	TAK	XML, CSV
5	dane o płatnikach i umowach,	Sybase	TAK	XML, CSV
6	dane statystyczne rozliczonych pacjentów do NFZ, dane wykonanych usług medycznych	Sybase	TAK	XML, CSV, format eksportu NFZ
7	dane opisowe	Sybase	TAK	XML, CSV
8	wyniki badań	Sybase	TAK	XML, CSV
9	Kolejki oczekujących	Sybase	TAK	XML, CSV

II.4.5 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 1 do OPZ 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.4.6 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.

W ramach konfiguracji środowiska systemu Zamawiający będzie odpowiedzialny za konfigurację, urządzeń sieciowych zgodnie z uzgodnionym projektem technicznym migracji. Za pozostałe prace w tym instalację i konfigurację serwerów, systemów operacyjnych, baz danych i aplikacji odpowiada Wykonawca.

Tabela: struktura baz danych wymagających migracji

L.P.	OPIS	SZCZEGÓŁY
1.	Ilość baz danych	2
2.	Rodzaj baz danych	złożona relacyjna
3.	Struktura poszczególnych baz danych	relacyjna
4.	Rodzaje i ilość tabel	tabele zgodne z bazą danych Sybase - 9890 tabel
5.	Zakres danych w tabelach	dane medyczne z lat 2008 - 2019
6.	Opis danych w tabelach	pacjenci, słowniki, dane rozliczeniowe, dane statystyczne, kolejki oczekujących
7.	Relacje pomiędzy danymi	w podmiocie medycznym przyjęto taką relację między danymi, że nigdy jedna informacja, nie jest zapisywana w bazie dwa razy
8.	Zainstalowane procedury po stronie serwera bazy danych	procedura bezpieczeństwa, procedura kontroli spójności danych
9.	Logiczne powiązania pomiędzy tabelami w bazie danych	brak
10.	Rozmiar baz danych	Są 4 instancje – CliniNet – 700GB, CliniNet-Psycho – 9GB, NetRAAD – 167GB, STER – 90GB,
11.	Sposób migracji	Do decyzji wykonawcy. Możliwość udostępnienia pliku csv, xls.
12.	Informacje na temat spójności danych	dane są spójne

II.4.7 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 appliance 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 eksportu 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 zbiór 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 polegać 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: <ul style="list-style-type: none"> • 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.4.8 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.4.9 Testy

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 przedwdrozeniowej
 - 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.

Dokumentacja z przeprowadzonych testów

Dokumentacja będąca podstawą przeprowadzenia testów zostanie opracowana przez Wykonawcę na etapie analizy przedwdrozeniowej. 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 jakiegokolwiek 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 wymienionego w Załączniku nr 1 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 wymienionego w Załączniku nr 1 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.

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 któregośkolwiek 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 wystąpienia 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 będzie 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 w opisie raportu z testów.

II.4.10 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 przeprowadzeniu procesu migracji testowej systemu na wydajniejszą bazę danych przedstawia raport z migracji wg szablonu uzgodnionego na etapie analizy przedwdrożeńowej 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 przedwdrożeńowej 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 przedwdrożeńowej.
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 będą 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

ture. 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 wstrzymać 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.4.11 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 Biura 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.4.12 Instruktaże

1. Zamawiający określa liczbę osób do odbycia instruktażu stanowiskowego dla nowo wdrażanych rozwiązań na maksymalnie 200 osób.
2. Zamawiający wymaga by w przypadku zmiany elementów interfejsu graficznego systemu (układ pól, inny układ formularzy itp.) i/lub przebiegu procesu (kolejność wykonywania działań, sposób i kolejność wywoływania formularzy itp.) w wyniku migracji Wykonawca był zobowiązany w tych obszarach przeszkolić liderów grup dziedzinowych po stronie Zamawiającego w ilości tożsamej z ilością migrowanych modułów dziedzinowych systemu i dostarczyć instrukcje oraz materiały szkoleniowe dla użytkowników systemu. Poprzez szkolenie liderów grup dziedzinowych personelu Zamawiający rozumie:
 - a) Instruktaże dla użytkowników końcowych Szpitalnego Systemu Informatycznego HIS. Instruktaże mają być przeprowadzone w siedzibie Zamawiającego w uzgodnionych terminach

tak by nie zakłóciły one bieżącej pracy. Za zgodą Zamawiającego dopuszczalne jest szkolenie poza siedzibą Zamawiającego. W takim przypadku Wykonawca ponosi koszty transportowe i zakwaterowania uczestników szkolenia. Instruktaż musi wyczerpywać zakres funkcjonalności niezbędnych do realizacji zadań wynikających z ról pracownika i nie może być krótszy niż 6 godz. Instruktaże powinny się odbywać w grupach max 12 osobowych. Wykonawca jest zobowiązany zapewnić sprzęt niezbędny do realizacji szkolenia. Zamawiający udostępni Wykonawcy salę szkoleniową na okres instruktaży i wymaga nie mniej niż 100 godzin szkoleniowych.

- b) W przypadku obowiązywania zasad i ograniczeń wynikających z rozporządzenia Ministra Zdrowia obostrzeń dotyczących zakazu zgromadzeń w związku z sytuacją epidemiologiczną COVID-19, Zamawiający dopuszcza przeprowadzenie instruktaży stanowiskowych on-line dla użytkowników oprogramowania SSI.
- c) Instruktaże stanowiskowe on-line powinny być prowadzone w technologii transmisji audio-video w czasie rzeczywistym, tzn. technologią typu „Streaming” umożliwiającą przesyłanie takich danych jak fonacja, wizja i tekst „na żywo” dzięki czemu uczestnik otrzymuje pełnowartościowe szkolenie:
- ✓ fonacja / głos – słyszy lektora prowadzącego szkolenie „na żywo”
 - ✓ wizja /video – 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 innymi uczestnikami instruktażu, poprzez:
- ✓ dostęp do czatu z możliwością zadawania pytań oraz udzielania odpowiedzi,
 - ✓ 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.
- d) 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.
- e) Instruktaże liderów poszczególnych modułów funkcjonalnych. Zamawiający oczekuje, że Wykonawca przeprowadzi pogłębione instruktaże dla użytkowników, którzy jako liderzy modułów będą stanowili wsparcie dla pozostałych użytkowników. Należy przewidzieć, że dla każdego z modułów Zamawiający wyznaczy po 2 liderów. Instruktaż musi trwać minimum 2 dni robocze (dodatkowe poza instruktażem użytkowników).
- f) Instruktaże administratora – instruktaże użytkownika(ów) wskazanych przez Zamawiającego do pełnienia funkcji administratora SSI, tj. instruktaż z administrowania systemem serwerowym

oraz bazodanowym, a także systemem wirtualizacji, konfiguracji, działania systemu w ilości 2 osób.

3. W ramach przeprowadzonych zajęć wymaga się:

- a) przekazania wiedzy niezbędnej do poprawnego użytkowania systemu, jego zakresu funkcjonalnego,
 - b) przekazania wiedza w zakresie tworzenia i gromadzenia informacji, tworzenia i gromadzenia dokumentów, wykonywania analiz, sprawozdań i raportów.
1. Wymaga się, by ww. instruktaże stanowiskowe odbyły się zgodnie z ustalonym harmonogramem wdrożenia.
 2. Obowiązkiem Wykonawcy będzie:
 - a) przeprowadzić instruktaże stanowiskowe z wdrażanych rozwiązań,
 - b) przygotować infrastrukturę instruktażową w udostępnionych salach (minimum: rzutnik full hd i ekran, a w razie potrzeby switch, serwer szkoleniowy, konfiguracja stanowisk),
 - c) uzyskać akceptację Zamawiającego co do zakresu i formy materiałów instruktażowych, przed udostępnieniem materiałów instruktażowych uczestnikom,
 - d) zapewnić każdemu uczestnikowi materiały instruktażowe,
 - e) zapewnić w trakcie instruktażu oraz w materiałach instruktażowych, oznakowanie zgodne z wytycznymi POPC informujące o współfinansowaniu projektu z UE,
 - f) sporządzić dokumentację papierową z przeprowadzonych instruktaży,
 - g) wszystkim uczestnikom instruktażu stanowiskowego i Administratora, po jego ukończeniu wystawić zaświadczenia

Harmonogramy szkoleń muszą umożliwiać pracownikom sekcji IT Zamawiającego obecność na zajęciach z danego tematu przeznaczonych dla innych grup zawodowych, z zastrzeżeniem, że na jednych zajęciach z danego tematu może być obecna co najwyżej połowa informatyków. tj. nie mniej 1 osoba.

Wykonawca nie ponosi odpowiedzialności za brak uczestnictwa użytkowników w instruktażach. Za skuteczne przeprowadzenie instruktażu uważa się dostępność w ustalonym miejscu i terminie przedstawicieli Wykonawcy, gotowych przeprowadzić instruktaż zgodnie z ustalonym harmonogramem.

Wykonawca w ramach instruktażu przekaze instrukcje do Systemu oraz materiały szkoleniowe.

Ilość godzin i sesji szkoleniowych nie jest ograniczona, jednakże muszą one się odbywać w okresie wdrożenia i zakończyć do podpisania protokołu zdawczo-odbiorczego.

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:

Infrastruktura serwerowa wraz z oprogramowaniem systemowym i narzędziowym:

POZ. SOPZ	OPIS	OKRES GWARANCJI (MINIMALNY)*
INFRASTRUKTURA SERWEROWA		

II.1.1	Serwer aplikacyjny	36 miesięcy
II.1.2	Serwer bazodanowy	36 miesięcy
II.1.3	Macierze	36 miesięcy
II.1.4	Pamięć masowa	36 miesięcy
II.1.5	Przełącznik FC	36 miesięcy
II.1.6	Przełączniki rdzeniowy sieci LAN	36 miesięcy
II.1.7	Przełącznik dostępowy sieci LAN typ 1	36 miesięcy
II.1.8	Przełącznik dostępowy sieci LAN typ 2	36 miesięcy
II.1.9	Punkty sieci bezprzewodowej	36 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.

2) Migracja bazy danych i wdrożenie Szpitalnego Systemu Informatycznego SSI:

POZ. SOPZ	OPIS	OKRES GWARANCJI (MINIMALNY)
SZPITALNY SYSTEM INFORMATYCZNY		
II.3.6	Migracja bazy danych System HIS – część medyczna	12 miesięcy
	System HIS, eUsługi – część medyczna – wdrożenie	12 miesięcy

2. Bieg terminów gwarancji określonych w ust. 1 będą rozpoczynać się z dniem podpisania Protokołu Odbioru Etapu lub Końcowego bez uwag przez Zamawiającego.

III.1 Usługi gwarancyjne

- W okresie gwarancji Wykonawca będzie zobowiązany do nieodpłatnego usuwania Wad Przedmiotu Zamówienia rozumianych jako Awaria lub Błąd lub Usterka zgodnie z definicjami jak poniżej:
 - Awaria** - Kategoria Wady w Oprogramowaniu lub Oprogramowaniu SSI lub Infrastrukturze Sprzętowej powodująca brak działania lub niepoprawne działanie Przedmiotu Zamówienia u Zamawiającego, uniemożliwiająca 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 lub Oprogramowania SSI oznaczającą jego funkcjonowanie niezgodne z opisem w Dokumentacji oraz OPZ, 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 Oprogramowaniu SSI lub Infrastrukturze Sprzętowej oznaczającą funkcjonowanie niezgodne z opisem Dokumentacji oraz OPZ, 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 aplikacyjny
- Serwer bazodanowy
- Macierz
- Pamięć masowa
- Przełącznik FC
- Punkty sieci bezprzewodowej

KWALIFIKACJA ZGŁOSZENIA WADY	OKRES DOSTĘPNOŚCI WYKONAWCY	ROZWIĄZANIE ZASTĘPCZE*	CZAS REAKCJI WYKONAWCY	CZAS NAPRAWY
AWARIA	24/7/365	niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 14 dni od czasu przyjęcia zgłoszenia
USTERKA		nie dotyczy	niezwłocznie nie później niż 5 dni roboczych od dnia przyjęcia zgłoszenia	niezwłocznie nie później niż 21 dni od dnia przyjęcia zgłoszenia

*Nie dotyczy wymiany sprzętu

Tabela 2. Usługi gwarancji dla Infrastruktury technicznej:

- Przełącznik rdzeniowy sieci LAN
- Przełącznik dostępowy sieci LAN typ 1
- Przełącznik dostępowy sieci LAN typ 2

KWALIFIKACJA ZGŁOSZENIA WADY	OKRES DOSTĘPNOŚCI WYKONAWCY	ROZWIĄZANIE ZASTĘPCZE	CZAS REAKCJI WYKONAWCY	CZAS NAPRAWY/WYMIANY
AWARIA	24/7/365	niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia
USTERKA		nie dotyczy	niezwłocznie nie później niż 5 dni roboczych od dnia przyjęcia zgłoszenia	niezwłocznie nie później niż 14 dni od dnia przyjęcia zgłoszenia

Tabela 2. Usługi gwarancji dla Szpitalnego Systemu Informatycznego

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	niezwłocznie, nie później niż 12 godzin od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 12 godzin od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia
BŁĄD		nie dotyczy	niezwłocznie nie później niż 2 dni robocze od dnia przyjęcia zgłoszenia	niezwłocznie nie później niż 3 dni roboczych od dnia przyjęcia zgłoszenia
USTERKA		nie dotyczy	niezwłocznie nie później niż 5 dni roboczych od dnia przyjęcia zgłoszenia	niezwłocznie nie później niż 10 dni roboczych od dnia przyjęcia zgłoszenia

- 2) dopuszcza się zmianę kwalifikacji zgłoszenia Wady, po uprzedniej zgodzie Zamawiającego. 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,

III.2 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 przekaze Wykonawcy, zgodnie ze stanem swojej wiedzy, informacje o aktach prawa wewnętrznego obowiązującego w Podmiocie leczniczym, które mają zastosowanie w realizacji niniejszej Umowy.
3. Usługi gwarancyjne na urządzenia muszą być świadczone przez producenta lub firmę autoryzowaną przez producenta lub jego przedstawiciela 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 świadczonej gwarancji dla Oprogramowania SSI i eUsług Wykonawca zobowiązuje się do:

- 1) wykonywania modyfikacji bez wezwania lub na pisemne zgłoszenie Zamawiającego w celu dostosowania wszystkich elementów Oprogramowania SSI i eUsług do obowiązujących przepisów prawnych,
- 2) przekazania Zamawiającemu informacji o nowych wersjach oprogramowania drogą elektroniczną na wskazany adres e-mail Zamawiającego,
 - 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 wraz z procedurą instalacji oprogramowania oraz informacją o parametryzacji i konfiguracji.
 - d) świadczenia usług w postaci konsultacji, porad 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.