

Załącznik Nr 1 do SIWZ

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. Zakres zamówienia

Zgodnie z założeniami projektu wynikającymi ze Studium Wykonalności, o nazwie: „Wdrożenie usług E-zdrowie w SSZZOZ im. dr. Teodora Dunina w Rudce”, realizowanego w ramach Regionalnego Programu Operacyjnego Województwa mazowieckiego na lata 2014-2020 (RPO WM 2014-2020), Oś Priorytetowa II: Wzrost e-potencjału Mazowsza, nr i nazwa Działania: 2.1 E-usługi, numer i nazwa Poddziałania: 2.1.1 E-usługi dla Mazowsza, Samodzielny Specjalistyczny Zespół Zakładów Opieki Zdrowotnej im. dr. Teodora Dunina znajdujący się przy Alei Teodora Dunina 1 w Rudce, 05-320 Mrozy, zamawia niżej wyszczególnione produkty i usługi, zgodnie z opisem poszczególnych elementów zamówienia, przedstawione poniżej.

Przedmiot zamówienia został podzielony na następujące Zadania, zgodne z Studium Wykonalności – „SW”, oraz Harmonogramem rzeczowo-finansowym – „HRF”:

1. Rozbudowa infrastruktury teleinformatycznej (HRF II.1)
 - a. Modernizacja i rozbudowa infrastruktury teleinformatycznej (SW 5.4.I.1)
 - i. rozbudowa oraz modernizacja istniejącego okablowania strukturalnego sieci komputerowej LAN (SW 5.4.I.1.1);
 - ii. modernizacja i rozbudowa części aktywnej sieci – przełączników (SW 5.4.I.1.2);
 - iii. przystosowanie pomieszczeń serwerowni do wymogów bezpieczeństwa przetwarzania i przechowywania danych (SW 5.4.I.1.3);
 - iv. rozbudowa systemów awaryjnego zasilania serwerów oraz sprzętu aktywnego w punktach dystrybucyjnych sieci komputerowej (SW 5.4.I.1.5);
 - b. Bezpieczeństwo systemu teleinformatycznego oraz przetwarzania danych (SW 5.4.I.2)
 - i. system kontroli styku sieci lokalnej LAN z Internetem – firewall nowej generacji (SW 5.4.I.2.1);
 - ii. system elektronicznej identyfikacji pacjentów (SW 5.4.I.2.2);
 - iii. archiwizacja danych (SW 5.4.I.2.3);
 - iv. ochrona antywirusowa (SW 5.4.I.2.4);
 - v. zapewnienie ciągłości pracy systemu (SW 5.4.I.2.5);
 - vi. uwierzytelnianie i autoryzacja użytkowników systemu (SW 5.4.I.2.6);
 - vii. zarządzanie zasobami systemu informatycznego (SW 5.4.I.2.7);
 - viii. oprogramowanie do zarządzania i monitorowania infrastruktury techniczną (SW 5.4.I.2.8).
2. Zakup sprzętu komputerowego (HRF II.2)
 - a. modernizacja użytkowanego sprzętu komputerowego – komputery stacjonarne, przenośne, urządzenia drukujące, skanery, w tym zakup nowych jednostek sprzętu (SW 5.4.I.1.6);

3. Budowa (rozbudowa) systemu EDM (HRF II.3)
 - a. Elektroniczna Dokumentacja Medyczna (EDM) (SW 5.4.I.3.4);
4. Modernizacja środowiska serwerowego (HRF II.4)
 - a. modernizacja użytkowanego środowiska przetwarzania danych – serwery, macierze, w tym zakup nowego wyposażenia (SW 5.4.I.1.4);
 - b. chmura obliczeniowa (SW 4.4)
 - c. oprogramowanie użytkowe (SW 5.4.I.3);
 - i. system oprogramowania obszaru medycznego – „część biała” (SW 5.4.I.3.1);
 - ii. system oprogramowania obszaru administracyjnego – „część szara” (SW 5.4.I.3.2);
 - iii. system wspomagania zarządzania – analizy BI (SW 5.4.I.3.3).
5. Wdrożenie e-usług (HRF II.5)
 - a. e – Rejestracja
 - b. e – Zgoda
 - c. e – Dokumentacja
 - d. e – Kontrahent
 - e. e – Wywiad
 - f. e – Kolejka
 - g. e – Identyfikacja
 - h. e – Powiadomienie
 - i. e – Informacja
6. Usługi wdrożeniowe (HRF II.6)
7. Usługi informatyczne (HRF II.7)
 - a. analiza przedwdrożeniowa, projekt techniczny systemu (SW 5.4.I.5.1);
 - b. instalacja, konfiguracja sieci komputerowej, środowiska serwerów, stacji roboczych (SW 5.4.I.5.2);
 - c. wdrożenie systemów oprogramowania, e-usług, szkolenia użytkowników (SW 5.4.I.5.3);
 - d. migracja danych do nowego systemu (SW 5.4.I.5.4);
 - e. integracja systemu z obszarami dziedzinowymi: diagnostyka obrazowa, gospodarka lekami (SW 5.4.I.5.5);
 - f. opieka powdrożeniowa, wsparcie użytkowników (SW 5.4.I.5.6);
 - g. audyt bezpieczeństwa wdrożonego systemu na zgodność z wymogami przepisów (SW 5.4.I.5.7).

2. Cele projektu

Głównym celem projektu jest stworzenie systemu e-usług publicznych z zakresu ochrony zdrowia świadczonych drogą elektroniczną, służących zwiększeniu wykorzystania technologii informacyjnych i komunikacyjnych (TIK) dla poprawy jakości usług zdrowotnych.

Cele szczegółowe projektu:

- a) zwiększanie liczby oraz jakości usług, udostępnianych w formie elektronicznej poprzez wykorzystanie nowoczesnych technologii informacyjnych i komunikacyjnych (TIK),

- b) wdrożenie elektronicznej dokumentacji medycznej (EDM), dostosowującej działalność Szpitala do znowelizowanych przepisów prawa,
- c) zapewnienie bezpieczeństwa wdrażanych systemów informatycznych oraz przetwarzania danych zgodnie z obowiązującym prawem,
- d) zapewnienie interooperacyjności z platformą krajową P1 lub P2 lub innymi rozwiązaniami funkcjonalnie odpowiadającymi.

Powyższe cele bezpośrednie przekładają się na szereg celów pośrednich w projekcie:

- a) rozwój e-usług o jak najwyższym stopniu dojrzałości, z których korzystać będą obywatele,
- b) poprawa dostępności do publicznej służby zdrowia dla mieszkańców województwa,
- c) usprawnienie procesu obsługi pacjenta,
- d) poprawa jakości świadczonych usług zdrowotnych.
- e) usprawnienie procesu gromadzenia danych i informacji,
- f) podniesienie poziomu bezpieczeństwa danych i informacji,
- g) przyspieszenie dostępu do danych i informacji,
- h) rozwój kompetencji kadry Szpitala.

3. Kontekst prawny

Infrastruktura i system objęty niniejszym postępowaniem obejmuje większą część działalności szpitala, w związku z czym zakres obowiązujących przepisów prawa do uwzględnienia jest bardzo szeroki. Istotnym czynnikiem determinującym zakres obowiązujących przepisów prawa jest również informatyzacja sektora publicznego oraz służby zdrowia przeprowadzana na szczeblu krajowym przez wprowadzenie obowiązkowej rejestracji Elektronicznej dokumentacji medycznej. Wobec powyższego Zamawiający wymaga, aby systemy dostarczone przez Wykonawcę spełniały wszelkie obowiązujące oraz wchodzące w życie do końca okresu świadczenia asysty powdrożeniowej przepisy prawa. W tej sytuacji, wskazane poniżej akty prawne, należy traktować jedynie jako akty podstawowe dotyczące przede wszystkim działalności i informatyzacji podmiotów leczniczych, których przepisy Wykonawca jest zobowiązany zastosować w dostarczonych systemach:

- Ustawa z dnia 27 sierpnia 2004 roku o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz.U. 2004 nr 210 poz. 2135 ze zm.),
- Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. 2015 poz. 636 ze zm.),
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2016 poz. 922 ze zm.),
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2004 Nr 100, poz. 1024),
- Rozporządzenie Ministra Zdrowia z dnia 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. 2014 poz. 177 ze zm.),
- Ustawa o dostępie do informacji publicznej (Dz.U. 2001 Nr 112 poz. 1198 z późn. zm.),
- Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz.U. z 2013 poz. 262 ze zm.),
- Ustawa z dnia 27 lipca 2001r. o ochronie baz danych (Dz.U. 2001 nr 128 poz. 1402 ze zm.),
- Ustawa z dnia 7 lipca 1994 r. - Prawo budowlane (Dz.U. 1994 Nr 89 poz. 414 ze zm.)
- Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w

postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012 poz. 526)

- Rozporządzenie Ministra Nauki i Informatyzacji z dnia 19 października 2005 r. w sprawie testów akceptacyjnych oraz badania oprogramowania interfejsowego i weryfikacji tego badania (Dz.U. 2005 nr 217 poz. 1836)
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie niezbędnych elementów struktury dokumentów elektronicznych (Dz.U. 2006 nr 206 poz. 1517)
- Rozporządzenie Ministra Infrastruktury z dnia 6 lutego 2003 r. w sprawie bezpieczeństwa i higieny pracy podczas wykonywania robót budowlanych (Dz.U. 2003 nr 47 poz. 401)
- Dyrektywa WE - numer 2006/95/WE w sprawie harmonizacji ustawodawstwa Państw Członkowskich odnoszących się do sprzętu elektrycznego przewidzianego do stosowania w określonych w granicach napięcia.
- PN-IEC 60364-... – Instalacje elektryczne w obiektach budowlanych.
- SEP-E-004 – Elektroenergetyczne i sygnalizacyjne linie kablowe. Projektowanie i budowa.
- Normami EIA/TIA 568 wraz z załącznikami TSB36
- Normami ISO/IEC 11801, EN55022 oraz EN55024 Montaż okablowania strukturalnego
- PN-EN 50130-5 Systemy alarmowe
- PN-EN 50131-1:2009 Systemy alarmowe. Systemy sygnalizacji włamania i napadu
- PN-EN 50131-6:2008 Systemy alarmowe - Systemy sygnalizacji włamania
- PN-EN 50133-1:2007 / A 1:2007 Systemy alarmowe - Systemy Kontroli Dostępu. Wymagania systemowe
- CLC/TS 50131-7:2003 Systemy sygnalizacji włamania
- Ustawa z dnia 22.08.1997r. o ochronie osób i mienia
- PN-B-02840:1991 - Ochrona przeciwpożarowa budynków - Nazwy i określenia
- PN-E-08106:1992 - Stopnie ochrony zapewniane przez obudowy (Kod IP)
- PN-IS08421-4 - Ochrona przeciwpożarowa - Terminologia – Wyposażenie gaśnicze
- PN-M-51004-1:1987 - Części składowe automatycznych urządzeń sygnalizacji pożarowej - Wprowadzenie
- BN 84/8984-10 Zakładowe sieci telekomunikacyjne wewnętrzne. Instalacje wewnętrzne. Ogólne wymagania.
- BN-88/8984-19 - Zakładowe sieci telekomunikacyjne przewodowe. Linie kablowe. Ogólne wymagania.
- PN-IEC 60364-5-52:2002 Instalacje elektryczne w obiektach budowlanych. Dobór i montaż wyposażenia elektrycznego. Oprzewodowanie.
- PN-IEC60364-6-61 Instalacje elektryczne w obiektach budowlanych. Sprawdzanie. Sprawdzanie odbiorcze.
- PN-EN 50173-1:2011 „Technika informatyczna. Systemy okablowania strukturalnego. Część 1: Wymagania ogólne”.
- PN-EN 50174-1:2010 „Technika informatyczna. Instalacja okablowania. Część 1: Specyfikacja i zapewnienie jakości.”
- PN-EN 50174-2:2010 „Technika informatyczna. Instalacja okablowania. Część 2: Planowanie i wykonawstwo instalacji wewnątrz budynków.”
- PN-EN 50174-3:2005 „Technika informatyczna. Instalacja okablowania. Część 3: Planowanie i wykonawstwo instalacji na zewnątrz budynków.”

- PN-EN 50346:2009 „Technika informatyczna. Instalacja okablowania - Badanie zainstalowanego okablowania”
- PN-ISO/IEC 17799 (kwiecień 2003) „Technika Informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji.”
- „ISO/IEC11801 oraz EN 50173 dla klasy E.

4. Szczegółowy opis parametrów minimalnych dla zadań przedmiotu zamówienia

Ad 1. Rozbudowa infrastruktury teleinformatycznej (HRF II.1)

a. Modernizacja i rozbudowa infrastruktury teleinformatycznej (SW 5.4.I.1)

i. rozbudowa oraz modernizacja istniejącego okablowania strukturalnego sieci komputerowej LAN (SW 5.4.I.1.1);

W celu osiągnięcia wysokiej efektywności realizacji zadań wykonywanych przez jednostkę konieczne jest zapewnienie infrastruktury niezbędnej do działania e-Uслуг, tj. infrastruktury teletechnicznej, okablowania sieciowego (LAN) oraz zasilania. Wspomniana infrastruktura powinna tworzyć środowisko do działania e-Uслуг, które będzie zapewniało ich wysoką dostępność, bezpieczeństwo i szybkość działania. W związku z powyższym istniejąca infrastruktura musi ulec modernizacji i rozbudowie, aby umożliwić szybką, bezpieczną i bezawaryjną realizację zadań.

Wykonawca przed przystąpieniem do prac musi te prace zaplanować i przedstawić do weryfikacji projekt wykonawczy. Zamawiający zaakceptuje projekt i na tej podstawie Wykonawca może dokonać montażu.

I. Zakres prac

Nazwa	Budynek główny	Budynek administracji	Budynek ZOL
Projekt okablowania systemu e-Identyfikacja	1 szt.		1 szt.
Okablowanie systemu e-Identyfikacja	1 kpl.		1 kpl.
Projekt LAN i EN		1 kpl.	
Okablowanie strukturalne LAN		1 kpl.	
Sieć elektryczna		1 kpl.	1 kpl.
PEL		24 szt.	
Modernizacja PD	4 szt.		
Instalacja PD	3 szt.	1 szt.	1 szt.
Szafa rack 18U	3 szt.		1 szt.
Szafa rack 22U		1 szt.	

Szafa rack 42U			2 szt.
Patchpanel	9 szt.	2 szt.	7 szt.
Organizator kabli	9 szt.	2 szt.	7 szt.
Przełącznica światłowodowa		1 kpl.	1 kpl.
Światłowód			1 kpl.
UPS typ I	7 szt.	1 szt.	1 szt.
Bezprzewodowy punkt dostępowy			1 szt.
System gaszenia serwerowni			1 kpl.
System monitoringu parametrów środowiskowych i kontroli dostępu			1 kpl.
Klimatyzacja			1 kpl.
Adaptacja pomieszczenia serwerowni			1 kpl.
Zasilanie serwerowni			1 kpl.

II. Wymagania w stosunku do przedmiotu zamówienia

1. Projekt okablowania systemu e-identyfikacji

Sporządzić projekt okablowania systemu e-identyfikacji dla danego budynku:

- nanieść na plan budynku rozmieszczenie elementów systemu e-identyfikacji;
- nanieść na plan budynku przebieg tras kablowych przy uwzględnieniu wskazówek Zamawiającego;
- oznaczyć projektowaną wielkość koryt PVC dla każdego odcinka trasy kablowej;
- nanieść projektowane oznaczenia kabli zgodnie z notacją uzgodnioną z Zamawiającym;
- uzyskać akceptację projektu Zamawiającego przed przystąpieniem do wykonywania prac;

2. Okablowanie systemu e-Identyfikacji

- wykonać na potrzeby połączenia elementów systemu e-identyfikacji z najbliższymi punktami dystrybucyjnymi;
- skrętka 4-parowa nieekranowana (U/UTP wg. ISO/IEC 11801/TIA) kategorii 5e w osłonie LSOH;
- kable poprowadzić w istniejących korytach PVC, w przypadku ich braku zainstalować brakujące koryta PVC;
- kable układać zachowując promień gięcia nie gorsze niż wymagania normy i specyfikacji producenta kabla;
- wykonanie zgodnie z niżej wymienionymi normami:
 - PN-EN 50173-1 „Technika informatyczna. Systemy okablowania strukturalnego. Część 1: Wymagania ogólne i strefy biurowe”;
 - PN-EN 50174-1 „Technika informatyczna. Instalacja okablowania. Część 1: Specyfikacja i zapewnienie jakości”;
 - PN-EN 50174-2 „Technika informatyczna. Instalacja okablowania. Część 2: Planowanie i wykonawstwo instalacji wewnątrz budynków”;
 - ISO/IEC11801 oraz EN 50173 dla klasy D.

3. Projekt LAN i EN

Sporządzić projekt sieci komputerowej i elektrycznej dla danego budynku:

- nanieść na plan budynku rozmieszczenie PEL zgodnie ze wskazówkami Zamawiającego w ilości wynikającej z tabeli *Zakres prac* dla danego budynku;
- nanieść na plan budynku przebieg tras kablowych przy uwzględnieniu wskazówek Zamawiającego;
- oznaczyć projektowaną wielkość koryt PVC dla każdego odcinka trasy kablowej;
- nanieść projektowane oznaczenia gniazd zgodnie z notacją uzgodnioną z Zamawiającym;
- zaprojektować wyposażenie rozdzielni elektrycznych i obwody elektryczne;
- uzyskać akceptację projektu Zamawiającego przed przystąpieniem do wykonywania prac;
- projekt w części elektrycznej powinien być sporządzony zgodnie z wymaganiami stosownych przepisów, norm i obowiązujących dobrych praktyk technicznych przez osoby posiadające stosowne uprawnienia;
- sporządzić dokumentację w zakresie niezbędnym do złożenia zgłoszenia robót budowlanych, przeprowadzić w imieniu Zamawiającego procedurę związaną ze zgłoszeniem robót budowlanych oraz dokonać wszelkich uzgodnień w jej toku;

4. Okablowanie strukturalne LAN

- wykonać zgodnie z Projektem LAN i EN na potrzeby połączenia PEL z PD;
- skrętka 4-parowa nieekranowana (U/UTP wg. ISO/IEC 11801/TIA) kategorii 6 w osłonie LSOH;
- kable poprowadzić w korytach PVC;
- kable układać zachowując promienie gięcia nie gorsze niż wymagania normy i specyfikacji producenta kabla;
- w przypadku współbieżnego prowadzenia okablowania sieci elektrycznej i komputerowej do punktów elektryczno-logicznych, okablowanie poprowadzić w korytach wielokomorowych zapewniających separację skrętki komputerowej od kabli elektrycznych;
- wykonać pomiary gniazd sieci komputerowej w celu potwierdzenia zgodności parametrów toru transmisyjnego ze stosownymi normami, raporty z pomiarów wygenerowane z urządzenia pomiarowego dostarczyć w formie elektronicznej;
- wykonanie zgodnie z niżej wymienionymi normami:
 - PN-EN 50173-1 „Technika informatyczna. Systemy okablowania strukturalnego. Część 1: Wymagania ogólne i strefy biurowe”;
 - PN-EN 50174-1 „Technika informatyczna. Instalacja okablowania. Część 1: Specyfikacja i zapewnienie jakości”;
 - PN-EN 50174-2 „Technika informatyczna. Instalacja okablowania. Część 2: Planowanie i wykonawstwo instalacji wewnątrz budynków”;
 - PN-EN 50346 „Technika informatyczna. Instalacja okablowania. Badanie zainstalowanego okablowania”;
 - PN-ISO/IEC 17799 (kwiecień 2003) „Technika Informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji.”;
 - ISO/IEC11801 oraz EN 50173 dla klasy E.

5. Sieć elektryczna

- wykonać zgodnie z Projektem LAN i EN;
- obwody elektryczne do gniazd elektrycznych w PEL wykonać przewodem 3-żyłowym o powierzchni co najmniej 2,5mm² w przekroju poprzecznym;

- sieć elektryczna musi posiadać ochronę przeciwzwarciovą i przeciwprzeciężeniową oraz spełniać wymagania ochrony przeciwporażeniowej;
- wykonać punkty połączeń wyrównawczych zgodnie z przynależnością pomieszczenia do grupy zagrożenia porażenia prądem elektrycznym zgodnie z wymaganiami normy;
- w ramach sieci elektrycznej wykonać modernizację rozdzielni elektrycznych w celu zgodnego z obowiązującymi przepisami i normami zabezpieczenia obwodów elektrycznych;

6. PEL

Zainstalować punkt elektryczno-logiczny składający się z:

- puszki natynkowej 3xM45 (3M) wraz z niezbędnym wyposażeniem;
- 2 x gniazdo sieci komputerowej 8P8C (RJ-45):
 - gniazda typu keystone kategorii 6 wg. ISO/IEC 11801/TIA dla kabla U/UTP;
 - zakończone zgodnie z T568B wg. TIA/EIA-568-B;
 - wyposażone w przesłonę przeciwkurzową;
 - każde gniazdo oznaczone zgodnie z notacją uzgodnioną z Zamawiającym;
- 2 x gniazdo elektryczne 2P+Z;

7. Modernizacja PD

- zainstalować w Punkcie Dystrybucyjnym w istniejącej szafie patchpanele Rack 19" (w ilości wynikającej z tabeli *Zakres prac*) modułarne z gniazdami 8P8C typu keystone:
 - tego samego rodzaju co w PEL - w przypadku Okablowania strukturalnego LAN;
 - kategorii 5e – w przypadku Okablowania systemu e-Identyfikacja;
- ilość gniazd keystone dostosować do ilości nowo instalowanego okablowania;
- zainstalować w istniejącej szafie organizatory kabli Rack 19" 19" (w ilości wynikającej z tabeli *Zakres prac*);
- dostarczyć i zainstalować patchcordsy U/UTP kategorii 6 wg. ISO/IEC 11801/TIA o długości 1m w liczbie równej liczbie nowo zainstalowanych gniazd w patchpanelach;
- nowo zainstalowane okablowanie w PD uporządkować i opisać zgodnie z notacją uzgodnioną z Zamawiającym;
- zainstalować UPS typ I (w ilości wynikającej z tabeli *Zakres prac*) i podłączyć do istniejącego gniazda zasilania;

8. Instalacja PD

- dostarczyć i zainstalować w Punkcie Dystrybucyjnym szafę Rack 19" (w ilości wynikającej z tabeli *Zakres prac*);
- zainstalować w szafie patchpanele Rack 19" (w ilości wynikającej z tabeli *Zakres prac*) modułarne z gniazdami 8P8C typu keystone:
 - tego samego rodzaju co w PEL - w przypadku Okablowania strukturalnego LAN;
 - kategorii 5e – w przypadku Okablowania systemu e-Identyfikacji;
- ilość gniazd keystone dostosować do ilości nowo instalowanego okablowania;
- zainstalować w szafie organizatory kabli Rack 19" 19" (w ilości wynikającej z tabeli *Zakres prac*);
- jeżeli w danej lokalizacji istniał PD przenieść jego zawartość do nowej szafy;
- dostarczyć i zainstalować patchcordsy U/UTP kategorii 6 wg. ISO/IEC 11801/TIA o długości 1m w liczbie równej liczbie nowo zainstalowanych gniazd w patchpanelach;

- nowo zainstalowane okablowanie w PD uporządkować i opisać zgodnie z notacją uzgodnioną z Zamawiającym;
- zainstalować UPS typ I (w ilości wynikającej z tabeli *Zakres prac*) i podłączyć do istniejącego gniazda zasilania;

9. Szafa rack 18U

- szafa wisząca ze stelażem Rack 19" o wysokości 18U;
- głębokość co najmniej 600mm;
- drzwi przednie – szklane z zamkiem;
- zdejmowane panele boczne;
- konstrukcja z blachy stalowej;
- wyposażona w:
 - szczotkowe przepusty kablowe;
 - co najmniej dwa wentylatory dachowe sterowane termostatem;
 - listwa zasilająca 8g. zamontowana w stelażu rack;
- maksymalne obciążenie szafy – co najmniej 40 kg;

10. Szafa rack 22U

- szafa stojąca ze stelażem Rack 19" o wysokości co najmniej 22U;
- głębokość co najmniej 600mm;
- drzwi przednie – szklane z zamkiem;
- zdejmowane panele boczne;
- konstrukcja z blachy stalowej;
- wyposażona w:
 - szczotkowe przepusty kablowe;
 - co najmniej dwa wentylatory dachowe sterowane termostatem;
 - listwa zasilająca 8g. zamontowana w stelażu rack;
- maksymalne obciążenie szafy – co najmniej 40 kg;

11. Szafa rack 42U

- skręcana szafa stojąca;
- wewnątrz stelaż Rack 19" o wysokości 42U złożony z przednich i tylnych profili montażowych;
 - regulowane położenie profili montażowych przednich i tylnych;
 - oznaczone i ponumerowane poziomy U;
- wymiary 800x1000mm (szerokość x głębokość);
- nośność co najmniej 500kg;
- przednie drzwi metalowe, perforowane;
- tylne drzwi metalowe;
- zdejmowane osłony boczne;
- dach i podłoga z możliwością wprowadzenia kabli i instalacji wentylatorów;
- wyposażona w:
 - uchwyty do pionowej organizacji kabli;
 - cokół;
 - szczotkowe przepusty kablowe;
 - panel wentylacyjny sterowany termostatem;

- 4 x listwa zasilająca 8g. zamontowana w stelażu rack;

12. Patchpanel

- montowany w stelażu rack 19”;
- miejsce na 24 porty typu keystone;
- metalowa tacka do przymocowania kabli;

13. Organizator kabli

- montowany w stelażu rack 19”;
- konstrukcja metalowa, metalowe uchwyty kabli;

14. Przełącznica światłowodowa

- metalowa, montowana w stelażu rack 19”;
- wysuwana teleskopowo;
- wyposażona w:
 - 12 x adapter światłowodowy duplex;
 - tacka spawów;
 - pigtaile;

15. Światłowód

- dostarczyć i zainstalować między serwerownią i PD;
- co najmniej 8 włókien;
- powłoka LSOH;
- zakończyć w przełącznicach światłowodowych;
- przeprowadzić pomiary toru światłowodowego;

16. UPS do szaf

- zasilacz awaryjny;
- moc wyjściowa co najmniej 1000VA;
- czas podtrzymania dla obciążenia 700 W – co najmniej 10 minut;
- typ: on-line (podwójna konwersja);
- napięcie wejściowe/wyjściowe 230V;
- zniekształcenia napięcia wyjściowego – mniej niż 3%;
- wbudowany układ obejścia (bypass);
- gniazdo wejściowe: IEC-320 C14;
- gniazda wyjściowe – co najmniej 6 x IEC 320 C13;
- porty komunikacyjne:
 - DB-9 RS232;
 - Ethernet;
- zarządzanie i monitoring:
 - telnet;
 - ssh;
 - przeglądarka internetowa;
 - obsługa IPv6;
 - Modbus TCP;
 - wyłączanie serwera przez sieć LAN;

- wielopoziomowy dostęp do zarządzania;
 - współpraca z radius;
- możliwość wymiany akumulatorów bez wyłączenia UPS;
- filtrowanie napięcia – ochrona przed przepięciami i impulsami elektrycznymi;
- automatyczne włączenia UPSa po powrocie zasilania;
- montaż do stelaża rack 19" (akcesoria montażowe w komplecie);
- wysokość – nie więcej niż 2U;
- oprogramowanie w komplecie;
- gwarancja co najmniej 2 lata;

17. Bezprzewodowy punkt dostępowy

- wyposażony w dwa interfejsy bezprzewodowe:
 - a/n;
 - b/g/n;
- obsługa 2x2 MIMO;
- port Ethernet 10/100/1000 Mbps;
- wbudowane anteny wewnętrzne;
- złącza do podłączenia anten zewnętrznych;
- zasilanie Power over Ethernet (IEEE 802.3af);
- certyfikat Wi-Fi;
- kompatybilny z istniejącym już kontrolerem HPE 850 Unified Wired-WLAN Appliance;

18. System gaszenia serwerowni

- kompletny system gaszenia pomieszczenia obejmujący:
 - centrala zarządzająca;
 - butle ze środkiem gaśniczym;
 - instalacja i dysze gaszące;
 - czujniki pożaru;
 - mechanizm ręcznego włączania/wyłączania gaszenia;
- możliwość wyboru trybu wyzwolenia gaszenia: z koincydencją lub bez;
- środek gaśniczy:
 - pozbawiony wpływu na warstwę ozonową;
 - bezpieczny dla człowieka i urządzeń elektronicznych;
 - przydatny do gaszenia pożarów klasy A, B, C, E, F;
 - ilość pozwalająca na skuteczne gaszenie w kubaturze pomieszczenia serwerowni;
- sygnalizacja stanu urządzenia:
 - alarm ostrzegawczy;
 - wyzwolenia środka gaśniczego;
 - uszkodzenie systemu;

19. System monitoringu parametrów środowiskowych i kontroli dostępu

- monitorowanie i sygnalizowanie nieautoryzowanego dostępu do pomieszczenia serwerowni:
 - rozbrajanie i uzbrajanie systemu przez czytnik zbliżeniowy;
 - czujnik otwarcia drzwi;
 - elektromagnes blokujący otwarcie drzwi;

- czujnik ruchu;
 - sygnalizator dźwiękowy;
- monitorowanie i sygnalizowanie parametrów środowiskowych:
 - temperatura;
 - pożar;
 - zalanie;
- przechowywanie zdarzeń przez co najmniej 30 dni;
- podtrzymanie zasilania z akumulatora;

20. Klimatyzacja

- o mocy cieplnej zapewniającej efektywne chłodzenie pomieszczenia serwerowni z uwzględnieniem mocy wydzielanej przez zainstalowane urządzenia, nie mniejszej niż 7 kW dla chłodzenia;
- składająca się z części wewnętrznej i zewnętrznej;
- bezprzewodowy pilot sterujący w komplecie;
- ruchomy dyfuzor kierunkowy (w płaszczyźnie pionowej i poziomej);
- przepływ powietrza przez jednostkę wewnętrzną co najmniej 1000m³/h;
- funkcje:
 - chłodzenie;
 - grzanie;
 - samoczynne oczyszczanie (w tym osuszanie);
- zakres temperatur zewnętrznych, przy których zachowana jest możliwość chłodzenia: -10°C ÷ 40°C;
- gwarancja co najmniej 2 lata z możliwością rozszerzenia do 5 lat;

21. Adaptacja pomieszczenia serwerowni

- dostosować pomieszczenie do potrzeb serwerowni;
- zamurować okno zewnętrzne, wraz z robotami wykończeniowymi;
- przenieść z pomieszczenia rurę kanalizacyjną;
- wykonać prace malarskie wraz z uzupełnieniem tynków;
- zamontować pod sufitem koryta metalowe w celu rozprowadzenia okablowania do szaf;
- dostosować drzwi wejściowe:
 - zamontować drzwi antywłamaniowe z atestowanymi z zamkami mechanicznymi przystosowanymi do systemu kontroli dostępu;
 - uzupełnić tynki przy otworze drzwiowym;
 - drzwi muszą mieć certyfikaty i atesty niezbędne dla ochrony pomieszczenia serwerowni;
- dostosować wentylację w związku z instalacją Systemu gaszenia serwerowni;

22. Zasilanie serwerowni

- doprowadzić zasilanie do serwerowni w budynku ZOL z rozdzielni głównej zlokalizowanej w budynku administracji:
 - wykonać wykop;
 - ułożyć trzy rury osłonowe o średnicy co najmniej 75 mm;
 - ułożyć kabel elektryczny 5 żyłowy;

- zabezpieczyć kanalizację taśmą ostrzegawczą;
- zasypać wykop i odtworzyć nawierzchnię;
- wykonać przepusty kablowe do wnętrza budynków, zgodnie z przepisami p.poż o odporności ogniowej minimum EI60;
- wewnątrz budynku zainstalować kabel elektryczny w listwach natynkowych PVC;
- zaprojektować i wykonać w pomieszczeniu serwerowni rozdzielnię oraz obwody elektryczne z zabezpieczeniami dla:
 - Zasilacz awaryjny UPS (dwa gniazda w szafie nr 1);
 - Klimatyzacja (dwa gniazda);
 - obwód zapasowy:
 - podwójne gniazdo w pomieszczeniu serwerowni;
 - po jednym podwójnym gnieździe w każdej szafie;
- wykonać projekty i dokumentację oraz przeprowadzić wymagane prawem procedury administracyjne niezbędne do wykonania prac;

Rozbudowa zostanie wykonana uwzględniając i rozszerzając obecnie funkcjonującą sieć, której projekt został umieszczony w Załączniku nr 3 do OPZ. W przypadku przekroczenia wartości progowych obciążenia prądowego, należy rozważyć budowę przyłącza energetycznego do wyłącznika głównego NN.

ii. modernizacja i rozbudowa części aktywnej sieci – przełączników (SW 5.4.1.1.2);

Dostawa: Przełącznik agregacyjny 10GbE - 2 szt.

Parametr	Charakterystyka (wymagania minimalne)
Producent	Nazwa producenta:
Identyfikacja	Typ produktu, model:
Ilość portów	<ul style="list-style-type: none"> - Min 24 porty 10 Gigabit Ethernet SFP+ SM - Możliwość instalacji wymiennie modułów <ul style="list-style-type: none"> a) 4 porty 10Gigabit Ethernet SFP+ lub b) 4 porty 10Gigabit Ethernet 10GBaseT lub c) 2 porty 40GbE (QSFP+) - 1 port RJ45 umożliwiający zarządzanie poprzez konsolę, - 1 port Ethernet RJ45 dedykowany do zarządzania Out-Of-Band - 1 port USB <p>Wszystkie porty muszą zostać wyposażone w odpowiednie wkładki. Rodzaj wkładek zostanie ustalony na podstawie analizy przedwdrożeniowej.</p>
Wymiar	<p>Szerokość: 19 cali do montażu w szafie rackowej,</p> <p>Wysokość: max 1 U</p> <p>Głębokość: max 48 cm</p>
Funkcjonalność	<ul style="list-style-type: none"> • Stakowalny do minimum 10 urządzeń w stosie portami 40GbE lub 10GbE (min 160Gbps) • Musi wspierać inny niż stackowanie mechanizm wielościeżki warstwy 2 na min.: 2 urządzeniach, umożliwiający budowę topologii sieci bez pętli.

- Możliwość obsługi modułów QSFP+ 40GE-SR4
- Możliwość obsługi modułów SFP+ co najmniej typów:
 - a) 10GBase-SR
 - b) 10GBase-LR
 - c) 10GBase-LRM
- Możliwość obsługi modułów SFP co najmniej typów:
 - d) 1000Base-SX
 - e) 1000Base-LX
 - f) 1000BaseT
- Możliwość obsługi kabli DAC 40GbE (Direct Attached Cable) min długości::
 - g) 0.5m
 - h) 1m
 - i) 3m
 - j) 5m
 - k) 7m
- Możliwość obsługi kabli DAC 10GbE (Direct Attached Cable) min długości::
 - l) 0.5m
 - m) 1m
 - n) 3m
 - o) 5m
 - p) 7m

W komplecie 3 sztuki kabli światłowodowych OM3 50/125 LC-SC o długości 2m każdy

- Możliwość obsługi kabli rozszywających DAC (Direct Attached Cable) 1 x 40GbE na 4 x 10GbE min długości:
 - q) 0.5m
 - r) 1m
 - s) 3m
 - t) 5m
 - u) 7m
- Redundantne min 2 zasilacze AC
- Redundantne min wiatraki
- Chłodzenie przełącznika od portów Eth w kierunku zasilaczy (od przodu do tyłu urządzenia)
- Forwarding Rate min. 470 Mpps
- Switching fabric min. 640 Gbps
- Wsparcie dla Jumbo Frame min 9KB
- Obsługa IPv6
- Obsługa PVST+ i RPVST+ lub technologii równoważnych
- Obsługa protokołów CDP lub równoważnych
- Obsługa routingu, min.:
 - RIP v1/2;
 - OSPF v1/2/3
- Obsługa multicastu, min.:

	<ul style="list-style-type: none"> - IGMP v1/2/3; - IGMP Snooping Querier - IGMP Proxy - PIM-SM i SSM <ul style="list-style-type: none"> • Rozmiar tablicy routingu min.: 8 000 wpisów IPv4, 4 000 wpisów IPv6 • Pamięć MAC adresów min. 130 000 • Wsparcie multicast, min 2000 Grup multicastowych • ACL – minimum 100 list, minimum 1000 reguł na ACL, min 4000 reguł na wszystkie ACL • Min 1000 aktywnych VLANów • Obsługa Prywatnych VLANów • Pobór mocy max 180 W
- Zarządzanie, zabezpieczenia	<ul style="list-style-type: none"> - Połączenie szyfrowane: SSL/SSH, - autentykacja dostępu do przełącznika w oparciu o Radius lub TACACS+ - listy dostępu (ACL) warstwy 2/3/4 - listy dostępu (ACL) konfigurowalne dla fizycznego portu, łącza zagregowanego LAG i VLAN - obsługa RMON, - obsługa SNMP v2 i v3, - obsługa sFlow, - możliwość przechowywania dwóch wersji oprogramowania na przełączniku, - obsługa DHCP Server i Relay Agent, - obsługa 802.1x w tym: <ul style="list-style-type: none"> a) MAC-based authentication b) MAC authentication bypass c) Guest VLAN - Zarządzenie przez CLI i przez przeglądarkę internetową, - Producent sprzętu powinien udostępnić darmowe oprogramowanie do centralnego zarządzania przełącznikami w ilości min 10 licencji.
Warunki gwarancji	<p>Gwarancja czasu życia (Limited Lifetime warranty) obejmująca:</p> <ul style="list-style-type: none"> - przełącznik - zasilacze i wiatraki - moduły SFP, SFP+ i QSFP+ - bezterminowy dostęp do nowych wersji oprogramowania <p>36 miesięcy gwarancji realizowanej w miejscu instalacji sprzętu z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, zgłaszanie 24x7x365, możliwość wydłużenia gwarancji producenta do 7 lat.</p> <p>Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta – dokumenty potwierdzające załączyć do oferty.</p> <p>Oświadczenie producenta, dostarczone do Umowy, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.</p>
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w wersji elektronicznej i drukowanej w języku polskim lub angielskim

Zamawiający posiada nieużywane wkładki SFP i SFP+, które wykonawca może wykorzystać w swoim rozwiązaniu. Zamawiający posiada 1 x SFP LC LX, 12x SFP LC SX, 2x SFP+ LC SR i 4x 10G SW iSCSI. W przypadku braku ich działania w zaproponowanej technologii przez Wykonawcę, Wykonawca musi dostarczyć do wszystkich urządzeń sieciowych światłowodowych, oferowanych w zamówieniu wszystkie wkładki SFP/SFP+ zgodnie z wymaganymi portami/połączeniami. Szczegółowa ilość niezbędnych wkładek zależy od zastosowanej przez Wykonawcę technologii oraz projektu wykonawczego sieci i zostanie ustalona na tym etapie. Należy założyć, że wszystkie porty muszą być obsadzone wkładkami, zarówno przy przełącznikach agregacyjnych jak i dostępowych, serwerach.

iii. przystosowanie pomieszczeń serwerowni do wymogów bezpieczeństwa przetwarzania i przechowywania danych (SW 5.4.I.1.3);

Pomieszczenie techniczne serwerowni jako centrum przetwarzania danych, musi spełniać szczególne warunki oraz zapewniać bezpieczeństwo w zakresie fizycznym jak i technicznym. Bezpieczeństwo techniczne musi zapewnić wyposażenie w urządzenia i systemy typu, będące przedmiotem zamówienia:

- system zasilania: rozdzielnie elektryczne, system dystrybucji mocy, system zasilania gwarantowanego UPS;
- system klimatyzacji i wentylacji: klimatyzacja, system wentylacji i przewietrzania po akcji gaśniczej;
- systemy bezpieczeństwa technicznego: system pożarowy – o najwyższym znaczeniu, system sygnalizacji włamania i napadu, system kontroli dostępu;

Prace adaptacyjne mają na celu zapewnienie odpowiednich warunków pracy dla serwerów, komputerów, urządzeń sieciowych, w które będą wyposażone obiekty Zamawiającego. Prace instalacyjne będą prowadzone i wykonywane w użytkowanym obiekcie. Wykonawca w porozumieniu z Użytkownikiem – Administratorem obiektu, zorganizuje prace w taki sposób, aby nie zakłócać normalnego i ciągłego działania Szpitala. Prace instalacyjne będą wykonywane w pomieszczeniu odseparowanym, wydzielonym na serwerownię oraz w pomieszczeniach pracy pracowników Szpitala.

iv. rozbudowa systemów awaryjnego zasilania serwerów oraz sprzętu aktywnego w punktach dystrybucyjnych sieci komputerowej (SW 5.4.I.1.5);

1. System zasilania

System zasilania gwarantowanego musi obejmować wszystkie systemy serwerowni. Zasilanie gwarantowane składać się będzie z:

- UPS 3kW w pomieszczeniu dotychczasowej serwerowni
- UPS 6kW w pomieszczeniu budowanej serwerowni
- Systemu automatycznego wyłączenia serwerów w trakcie utraty warunków zasilania
- Przyłącza energetycznego
- Skrzynki bezpiecznikowej

Nazwa komponentu	Wymagane minimalne parametry techniczne
------------------	---

Budowa	Modułowa
Moc znamionowa	Min. 3kW i 6kW
Funkcjonalność modułów mocy	Wymiana modułów mocy i/lub rozbudowa mocy UPSa bez konieczności przechodzenia na by-pass (przy zachowanie pracy online), tzw. HotSwap
Funkcjonalność	Awaryjne wyłączenia zasilania, Możliwość wyłączania urządzeń zewnętrznych np. serwerów w przypadku utraty mocy Współdziałanie z SZR i Agregatem Kompensacja mocy biernej Napięcie 230V AC 50Hz Instalacja w RACK lub wolnostojąca Online double conversion Możliwość modułowej rozbudowy o dodatkowe baterie Zimny start
Czas podtrzymania	Do momentu stabilizacji agregatu + 10min.
Rozłączniki manewrowe	Zasilacz UPS powinien być wyposażony w komplet rozłączników pozwalających na bezpieczne włączenie i wyłączenie UPSa.
Podłączenie zasilania i odbiorów	Podłączenie okablowania od tyłu zasilacza, z możliwością podłączenia dwóch oddzielnych torów do zasilania prostownika i bypassu wewnętrznego.
Normy	BSMI, EN/IEC 62040-2, EN/IEC 62040-1-1, VDE, PEP, EOLI, RoHS, CE
Instrukcja w języku polskim	Wymagane
Gwarancja	36 miesięcy na cały system UPS+baterie
Przeglądy	Wymagane przeglądy raz na rok wliczone w ofertę.

2. Przełącznik 1GbE PoE – 10 szt.

Komponent	Minimalne wymagania
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn, wyposażona w zintegrowany zasilacz Hot Plug.
Porty	Minimum 48 porty GigabitEthernet w standardzie BaseT z obsługą PoE+, minimum 4 zintegrowane porty 10Gb Ethernet SFP+, możliwość dedykowania dwóch portów 10Gb Ethernet SFP+ w celu połączenia przełączników w stos, minimum 1 port USB do konfiguracji przełącznika, 1 port RJ45 do portu konsoli wraz z odpowiednim kablem RJ45-RS232, wraz z wkładkami.
Wydajność przełącznika	- Minimum 16000 adresów MAC - switch fabric capacity min. 176Gbps w trybie full-duplex) - forwarding rate min. 164Mbps

	<ul style="list-style-type: none"> - pamięć flash min. 256MB - bufor pamięci dla pakietów minimum 1.5MB - pamięć procesora minimum 1GB - obsługa minimum 512 wirtualnych sieci - możliwość połączenia w stos do 8 urządzeń tego samego typu
Zgodność z protokołami	<p>802.1AB LLDP 802.1D Bridging, Spanning Tree 802.1p Ethernet Priority (User Provisioning and Mapping) 802.1Q VLAN Tagging, Double VLAN Tagging, GVRP 802.1S Multiple Spanning Tree (MSTP) 802.1v Protocol-based VLANs 802.1W Rapid Spanning Tree (RSTP) BPDU guard, BPDU filtering 802.1X Network Access Control, Auto VLAN 802.2 Logical Link Control 802.3 10BASE-T 802.3ab Gigabit Ethernet (1000BASE-T) 802.3ac Frame Extensions for VLAN Tagging 802.3ad Link Aggregation with LACP 802.3ae 10 Gigabit Ethernet (10GBASE-X) 802.3AX LAG Load Balancing 802.3az Energy Efficient Ethernet (EEE) 802.3u Fast Ethernet (100BASE-TX) on Management Ports 802.3x Flow Control 802.3z Gigabit Ethernet (1000BASE-X) ANSI LLDP-MED (TIA-1057) MTU 9,216 byte</p>
Zarządzanie siecią i bezpieczeństwo	<p>1155 SMIPv1 1157 SNMPv1 1212 Concise MIB Definitions 1213 MIB-II 1215 SNMP Traps 1286 Bridge MIB 1442 SMIPv2 1451 Manager-to-Manager MIB 1492 TACACS+ 1493 Managed Objects for Bridges MIB 1573 Evolution of Interfaces 1612 DNS Resolver MIB Extensions 1643 Ethernet-like MIB 1757 RMON MIB 1867 HTML/2.0 Forms with File Upload Extensions</p>

	1901 Community-based SNMPv2
	1907 SNMPv2 MIB
	1908 Coexistence Between SNMPv1/v2
	2011 IP MIB
	2012 TCP MIB
	2013 UDP MIB
	2068 HTTP/1.1
	2096 IP Forwarding Table MIB
	2233 Interfaces Group using SMIv2
	2246 TLS v1
	2271 SNMP Framework MIB
	2295 Transport Content Negotiation
	2296 Remote Variant Selection
	2346 AES Ciphersuites for TLS
	2576 Coexistence Between SNMPv1/v2/v3
	2578 SMIv2
	2579 Textual Conventions for SMIv2
	2580 Conformance Statements for SMIv2
	2613 RMON MIB
	2618 RADIUS Authentication MIB
	2620 RADIUS Accounting MIB
	2665 Ethernet-like Interfaces MIB
	2674 Extended Bridge MIB
	819 RMON MIB (groups 1, 2, 3, 9)
	2863 Interfaces MIB
	2865 RADIUS
	2866 RADIUS Accounting
	2868 RADIUS Attributes for Tunnel Prot.
	2869 RADIUS Extensions
	3410 Internet Standard Mgmt. Framework
	3411 SNMP Management Framework
	3412 Message Processing and Dispatching
	3413 SNMP Applications
	3414 User-based security model
	3415 View-based control model
	3416 SNMPv2
	3418 SNMP MIB
	3577 RMON MIB
	3580 802.1X with RADIUS
	3737 Registry of RMOM MIB
	4086 Randomness Requirements
	4113 UDP MIB
	4251 SSHv2 Protocol
	4252 SSHv2 Authentication

	4253 SSHv2 Transport 4254 SSHv2 Connection Protocol 4419 SSHv2 Transport Layer Protocol 4521 LDAP Extensions 4716 SECSH Public Key File Format
Warunki pracy	-Wydajność pracy zasilaczy na poziomie min. 80% - temperatura pracy w zakresie od 0 do 45 stopni celcjusza - wilgotność dla trybu pracy 85%
Certyfikaty i standardy	Zamawiający wymaga aby oferowany przełącznik: - został wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001 (dokumenty załączyć do oferty) - posiadał deklarację CE (dokument załączyć do oferty) - jest zgodny z standardem RoHS (oświadczenie producenta lub przedstawiciela producenta załączyć do oferty)
Gwarancja	Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Możliwość rozszerzenia gwarancji producenta do siedmiu lat.

Zamawiający posiada nieużywane wkładki SFP i SFP+, które wykonawca może wykorzystać w swoim rozwiązaniu. Zamawiający posiada 1 x SFP LC LX, 12x SFP LC SX, 2x SFP+ LC SR i 4x 10G SW iSCSI. W przypadku braku ich działania w zaproponowanej technologii przez Wykonawcę, Wykonawca musi dostarczyć do wszystkich urządzeń sieciowych światłowodowych, oferowanych w zamówieniu wszystkie wkładki SFP/SFP+ zgodnie z wymaganymi portami/połączeniami. Szczegółowa ilość niezbędnych wkładek zależy od zastosowanej przez Wykonawcę technologii oraz projektu wykonawczego sieci i zostanie ustalona na tym etapie. Należy założyć, że wszystkie porty muszą być obsadzone wkładkami, zarówno przy przełącznikach agregacyjnych jak i dostępowych, serwerach.

b. Bezpieczeństwo systemu teleinformatycznego oraz przetwarzania danych (SW 5.4.1.2)

i. system kontroli styku sieci lokalnej LAN z Internetem – firewall nowej generacji (SW 5.4.1.2.1);

W ramach realizacji Zamówienia dostawca dostarczy i uruchomi system bezpieczeństwa zapewniający wszystkie wymienione poniżej funkcje bezpieczeństwa niezależnie od dostawcy łącza Internet. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych zamkniętych platform sprzętowych lub w postaci komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System musi zostać połączony w klaster online – failover i klaster niezawodnościowy.

PARAMETR MINIMALNY

Całość dostarczanego sprzętu i oprogramowania pochodzi z autoryzowanego kanału sprzedaży producentów na terenie Unii Europejskiej
Oferowane urządzenia są nowe (tzn. wyprodukowane nie wcześniej niż na 6 miesięcy przed upływem terminu składania ofert) i nieużywane. <i>Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem, wyłącznie przez wykonawcę i wyłącznie w celu weryfikacji działania urządzenia. W takiej sytuacji Wykonawca zobowiązany będzie do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający będzie miał prawo do inspekcji sprzętu przed jego rozpakowaniem.</i>
Na żądanie Zamawiającego, na etapie badania i oceny ofert, zostaną przedstawione testy poszczególnych funkcjonalności
Oferowane urządzenia na dzień złożenia oferty nie są przeznaczone przez producenta do wycofania z produkcji lub sprzedaży
System zabezpieczeń firewall będzie dostarczony jako dedykowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze sprzętowej systemu będą istnieć mechanizmy zabezpieczające, które gwarantują niezmienną wydajność obsługi urządzenia poprzez interfejs do zarządzania oraz raportów bez względu na obciążenie wynikające z obsługiwanego ruchu sieciowego.
System zabezpieczeń firewall nie posiada ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej
Gwarantowana przepływność urządzenia dla funkcjonalności statefull firewalla z uruchomioną funkcją kontroli aplikacji $\geq 400\text{Mbit/s}$
Gwarantowana przepływność urządzenia dla funkcjonalności kontroli treści (anty-wirus AV, anty-spyware AS, IPS i web filtering URL) $\geq 150\text{Mbit/s}$
Liczba interfejsów 10/100/1000 Mbps min. 8 szt.
System zabezpieczeń firewall działa w trybie routera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer). Funkcjonując w trybie transparentnym urządzenie nie posiada skonfigurowanych adresów IP na interfejsach sieciowych jak również nie wprowadza segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA. Tryb pracy zabezpieczeń musi być ustalany w konfiguracji interfejsów inspekcyjnych.
System zabezpieczeń firewall ma możliwość pracy w trybie transparentnym (bez konieczności nadawania adresu IP) oraz pozwalać na tworzenie transparentnych subinterfejsów, które będą obsługiwały ruch z wybranych vlanów lub podsieci IP.
System zabezpieczeń firewall obsługuje protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie przełącznika i routera. Urządzenie musi obsługiwać 4094 znaczników VLAN.
Urządzenie obsługuje protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF.
System zabezpieczeń firewall zgodnie z ustaloną polityką prowadzi kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji.
Polityka zabezpieczeń firewall uwzględnia strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie

zdarzeń i alarmowanie oraz zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ).
System zabezpieczeń firewall automatycznie identyfikuje aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji odbywa się co najmniej poprzez sygnatury i analizę heurystyczną.
Identyfikacja aplikacji nie wymaga (choć może dopuszczać) podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji.
Konfiguracja dostępu do aplikacji odbywa się w jednolitym, zbiorczym interfejsie reguł dla polityki firewall (tzn. reguła firewall posiada oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowanie aplikacji przez dodatkowe profile). Nie jest dopuszczalna konfiguracja kontroli aplikacji w innych niezależnych modułach zarządzania (np. w IPS lub innym module UTM).
Liczba aplikacji wykrywanych przez System zabezpieczeń firewall (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS ≥ 2000
System zabezpieczeń firewall posiada możliwość ręcznego tworzenia sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
System zabezpieczeń firewall musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur aplikacji (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa.
System zabezpieczeń firewall umożliwia blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku odbywa się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.
System zabezpieczeń firewall zapewnia inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System ma możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.
System zabezpieczeń firewall umożliwia inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
System zabezpieczeń firewall ma możliwość transparentnego ustalenia tożsamości użytkowników sieci (integracja z Active Directory, Ms Exchange, Citrix, LDAP i serwerami Terminal Services). Polityka kontroli dostępu (firewall) precyzyjnie definiuje prawa dostępu użytkowników do określonych usług sieci i jest utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości odbywa się również transparentnie. Ponadto system ma możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.
System zabezpieczeń firewall posiada możliwość uruchomienia modułu filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza web filtering jest przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i posiada nie mniej niż 20 milionów rekordów URL.

System zabezpieczeń firewall musi być dostarczony z modułem filtrowania stron URL per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcjonalność filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). Minimalny czas trwania subskrypcji modułu musi wynosić 60 miesięcy
System zabezpieczeń firewall posiada możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.
System zabezpieczeń firewall musi posiadać możliwość automatycznego pobierania listy stron WWW z zewnętrznego systemu w określonych przedziałach czasu i używania ich w politykach bezpieczeństwa.
System zabezpieczeń firewall musi być dostarczony z modułem inspekcji antywirusowej AV per aplikacja oraz wybrany dekodery takie jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus jest przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzi od tego samego producenta co producent systemu zabezpieczeń. Minimalny czas trwania subskrypcji modułu musi wynosić 36 miesięcy.
System zabezpieczeń firewall posiada możliwość uruchomienia modułu inspekcji antywirusowej per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby moduł inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
System zabezpieczeń firewall musi być dostarczony z modułem wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS jest przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzi od tego samego producenta co producent systemu zabezpieczeń. Minimalny czas trwania subskrypcji modułu musi wynosić 60 miesięcy.
System zabezpieczeń firewall posiada możliwość uruchomienia modułu IPS/IDS per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcjonalność IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
System zabezpieczeń firewall posiada możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
System zabezpieczeń firewall musi być dostarczony z modułem anty-spyware AS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware jest przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzi od tego samego producenta co producent systemu zabezpieczeń. Minimalny czas trwania subskrypcji modułu musi wynosić 36 miesięcy.
System zabezpieczeń firewall posiada możliwość uruchomienia modułu anty-spyware per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcjonalność anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
System zabezpieczeń firewall posiada możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
System zabezpieczeń firewall musi posiadać możliwość definiowania i przydzielania różnych profili ochrony (AV, IPS, AS, URL, blokowanie plików) per aplikacja. Musi istnieć możliwość przydzielania

innych profili ochrony (AV, IPS, AS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.
System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe.
System zabezpieczeń firewall posiada funkcjonalność podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem.
System zabezpieczeń firewall posiada funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.
System zabezpieczeń firewall wykonuje statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT umożliwiają co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
System zabezpieczeń firewall musi posiadać osobny zbiór polityk, definiujący który ruch należy poddać funkcji NAT. Funkcjonalność NAT nie może być powiązana z politykami bezpieczeństwa.
System zabezpieczeń firewall posiada funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
System zabezpieczeń firewall umożliwia zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN odbywa się w oparciu o ustawienia routingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych odbywa się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji.
Maksymalna wydajność szyfrowania IPSec $\geq 100\text{Mbit/s}$
Maksymalna ilość obsługiwanych jednocześnie tuneli IPSec typu site-to-site ≥ 20
Maksymalna ilość obsługiwanych jednocześnie sesji VPN dla użytkowników ≥ 20
System zabezpieczeń firewall wykonuje zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System umożliwia stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego.
System zabezpieczeń firewall umożliwia integrację w środowisku wirtualnym VMware w taki sposób, aby firewall mógł automatycznie pobierać informacje o uruchomionych maszynach wirtualnych (np. ich nazwy) i korzystać z tych informacji do budowy polityk bezpieczeństwa. Tak zbudowane polityki skutecznie klasyfikują i kontrolują ruch bez względu na rzeczywiste adresy IP maszyn wirtualnych i jakkolwiek zmiana tych adresów nie pociąga za sobą konieczności zmiany konfiguracji polityk bezpieczeństwa firewalla.
Zarządzanie systemem zabezpieczeń odbywa się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem.
System zabezpieczeń firewall jest wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).

Dostęp do urządzenia i zarządzanie z sieci jest zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń pozwala na zdefiniowanie wielu administratorów o różnych uprawnieniach.
System zabezpieczeń firewall umożliwia uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS i Kerberos.
System zabezpieczeń firewall umożliwia stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).
System zabezpieczeń firewall posiada wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 30 GB. Wszystkie narzędzia monitorowania, analizy logów i raportowania są dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji.
Włączenie logowania na dysk nie obniża wydajności urządzenia.
System zabezpieczeń firewall posiada możliwość konfigurowania różnych serwerów Syslog per polityka bezpieczeństwa.
System zabezpieczeń firewall ma możliwość korelowania zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane zawierają informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i filtrowaniu stron WWW.
System zabezpieczeń firewall ma możliwość tworzenia wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów jest dostępny w formatach co najmniej PDF, CSV i XML.
System zabezpieczeń firewall ma możliwość stworzenia raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.
System zabezpieczeń firewall ma możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive. Moduł ochrony przed awariami monitoruje i wykrywa uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.
System zabezpieczeń firewall musi posiadać koncept konfiguracji kandydackiej którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu.
Czas gwarancji na dostarczany sprzęt liczony od daty odbioru systemu min 36 miesięcy.
Całość dostarczonego sprzętu jest objęta gwarancją, w okresie wymaganym przez Zamawiającego
Opieka techniczna przez okres trwania gwarancji. Opieka będzie zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną, wymianę uszkodzonego sprzętu, dostęp do nowych wersji oprogramowania, aktualizację bazy ataków IPS, definicji wirusów, filtracji adresów URL a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.
Naprawa lub wymiana urządzeń lub ich części, zgodnie z metodyką i zaleceniami producenta.

ii. system elektronicznej identyfikacji pacjentów (SW 5.4.I.2.2);

Wielozadaniowy system identyfikacji, monitoringu oraz lokalizacji Pacjenta

Obszar	Treść wymagania minimalnego
	1. URZĄDZENIA DO TRANSMISJI DANYCH
	Rejestrator Bluetooth – min 270 szt.
Funkcjonalność	Oprogramowanie konfigurowalne ze stacją roboczą
Funkcjonalność	Wbudowany przycisk przywołania
Funkcjonalność	Moc z jaką urządzenie pracuje: w zakresie od -18dBm do +8dBm
Funkcjonalność	Zasięg do 200m w otwartej przestrzeni
Funkcjonalność	Identyfikacja urządzenia numerem unikalnym MAC oraz tagiem NFC
Funkcjonalność	Włączanie/wyłączanie alarmu spowodowanego ruchem lub zmianą położenia
Funkcjonalność	Rodzaj archiwizowanych informacji: obecność w strefach oraz alarmy akcelerometru
Funkcjonalność	Hasło dostępu do urządzenia
Zasilanie	Bateria CR2032 (przybliżony czas działania min1 rok)
Obudowa	Plastik IP54
Pozostałe	Możliwość zdalnej wymiany oprogramowania
Pozostałe	Temperatura pracy: od 0°C do 65°C
Pozostałe	Opaska silikonowa na nadgarstek z możliwością montażu „zegarek”
	Transmitter GSM min 15 szt
Funkcjonalność	Parametry Bluetooth konfigurowalne ze stacją roboczą
Funkcjonalność	Rodzaj archiwizowanych informacji
Zasilanie	baterijne
GSM	Transmisja danych: GPRS
Pozostałe	Możliwość zdalnej wymiany oprogramowania
Pozostałe	Obsługa danych historycznych z rejestratorów
	Transmitter Ethernet min 100 szt
Funkcjonalność	Parametry konfigurowalne ze stacją roboczą
Funkcjonalność	Rodzaj przesyłanych informacji
Zasilanie	Wewnętrzny zasilacz 5V 500mA lub PoE
Pozostałe	Możliwość zdalnej wymiany oprogramowania
	Czytnik biurkowy Bluetooth: min 3 szt.
Funkcjonalność	Oprogramowanie konfigurowalne ze stacją roboczą
Funkcjonalność	Identyfikacja urządzenia numerem unikalnym MAC
Funkcjonalność	API do współpracy z przeglądarką oraz zintegrowaną aplikacją telemetryczną
Zasilanie	USB
Obudowa	Plastik min. IP54
Pozostałe	Możliwość zdalnej wymiany oprogramowania
	2. URZĄDZENIA I APLIKACJA ANDROID
	Smartfon Android min 10 szt.
Parametry	Wyświetlacz: min 4” pojemnościowy
Parametry	Procesor: min. 1,00 GHz;
Parametry	Waga: max 135g
Parametry	Zakres temperatury pracy: -10 to +45°C

Parametry	Zakres wilgotności: 0-75%
Zasilanie	Bateria: min. 1700 mAh
Pozostałe	Czas pracy: 6 h
Pozostałe	RAM: min. 512 MB
Pozostałe	Pamięć wewnętrzna: 4GB
Monitor dotykowy dla dyżurek pielęgniarek – min 5 szt.	
Parametry	<p>Procesor min. 4 rdzenie</p> <p>Pamięć RAM min. 8 GB (SO-DIMM DDR3, 1600 MHz)</p> <p>Typ ekranu Błyszczący, Dotykowy, LED</p> <p>Przekątna ekranu min.21"</p> <p>Rozdzielczość ekranu min.1920 x 1080 (FullHD)</p> <p>Dysk twardy min 500GB</p> <p>Łączność Bluetooth Wi-Fi 802.11 n/ac LAN 10/100/1000 Mbps</p> <p>Zasilacz min 120 W</p> <p>Zainstalowany okienkowy system operacyjny</p> <p>Gwarancja 36 miesięcy (gwarancja producenta)</p>
3. PLATFORMA TELEMETRYCZNA	
Funkcjonalność podstawowa	Rejestracja lokalizacji Pacjentów w 100 strefach
Funkcjonalność podstawowa	Prezentacja informacji podstawowej o Pacjencie (Integracja z HIS)
Funkcjonalność podstawowa	Prezentacja graficzna obecności Pacjentów w strefach
Funkcjonalność podstawowa	Wyszukiwanie Pacjentów w Szpitalu.
Funkcjonalność podstawowa	Monitorowanie aktywności fizycznej Pacjenta
Funkcjonalność podstawowa	Monitorowanie obecności Pacjenta w strefach
Funkcjonalność podstawowa	Monitorowanie obecności Pacjenta w strefach zakazanych
Funkcjonalność podstawowa	Alarmowanie o braku Pacjenta w strefie
Funkcjonalność podstawowa	Alarmowanie o braku aktywności
Funkcjonalność podstawowa	Alarmowanie o upadku, uderzeniu
Funkcjonalność podstawowa	Alarmowanie na dowolny telefoniczny nr wewnętrzny
Funkcjonalność podstawowa	Raportowanie historii pobytu Pacjenta w szpitalu
Funkcjonalność podstawowa	Raportowanie historii pobytu Pacjentów w strefach

Funkcjonalność podstawowa	Administracja aplikacją z poziomu stacji roboczej
Funkcjonalność podstawowa	Konfigurowalne role użytkowników: Administrator, Użytkownik
Funkcjonalność podstawowa	Konfigurowalne uprawnienia do przeglądania stref
Funkcjonalność podstawowa	Brak licencji na stacje robocze
Architektura	Aplikacja serwerowa dla systemu Windows lub Linux (w przypadku systemu Linux Wykonawca musi zapewnić licencje na ten system w przestrzeni zwirtualizowane serwerów dostarczanych w niniejszym zamówieniu)
Architektura	Możliwa praca w Intranecie oraz Internecie
Architektura	Możliwość backupu danych
Architektura	Obsługa ruchu danych przychodzących z sieci LAN oraz Internetu i sieci GSM
Architektura	Serwis Integracyjny z HIS działającym w szpitalu (wymiana danych identyfikacyjnych oraz danych podstawowych o Pacjencie)
Architektura	Serwis Integracyjny z aplikacją Android (alarmowanie, udostępnienie danych o Pacjencie)

Obszar	Treść wymagania
	System automatycznego trasowania połączeń dla systemu e-identyfikacja
Konfiguracja systemu	Linie wewnętrzne:
Konfiguracja systemu	- min 72 linie telefoniczne analogowe z funkcją CLIP w standardzie FSK
Konfiguracja systemu	- min 6 linii telefonicznych systemowych do podłączenia 1-parowych aparatów zaawansowanych
Konfiguracja systemu	- min 40 linii IP wewnętrznych dla przenośnych aparatów WLAN
Konfiguracja systemu	Linie zewnętrzne:
Konfiguracja systemu	- min 10 linii SIP Trunk Channel (podłączenie operatora VoIP)
Konfiguracja systemu	- min 8 linii miejskich analogowych (podłączenie operatora)
Wymagania systemu	Skalowalność docelowa wewnętrzna systemu: 200 linii TDM/300 terminali IP (tylko poprzez dokładanie kart, nie dopuszcza się sieciowania systemów)
Wymagania systemu	Zapowiedzi głosowe na dowolnych numerach zewnętrznych oddzielnie dla trybu pracy dzień/noc, zapowiedzi wgrywane z pliku w formacie WAV
Wymagania systemu	Wbudowany interfejs VoIP z minimum 40 jednoczesnymi kanałami głosowymi, możliwość rozbudowy interfejsu VoIP do minimum 100 kanałów rozmównych poprzez dołożenie modułu integrującego się z płytą główną
Wymagania systemu	Przystosowany zarówno do montażu wolnostojącego, jak i w szafie RACK 19"
Wymagania systemu	Dostarczany sprzęt musi być fabrycznie nowy z najnowszym oprogramowaniem, dotychczas nieużywany wyprodukowany nie wcześniej niż w 2016 roku, pochodzący z legalnego kanału sprzedaży producenta, przeznaczony na rynek polski; zamawiający zastrzega sobie możliwość zweryfikowania pochodzenia sprzętu

Wymagania systemu	Objęty minimum 24-miesięczną gwarancją z bezpłatnym dostępem do najnowszych aktualizacji oprogramowania w okresie 36 miesięcy (tzw. Software Support)
Wymagania systemu	Musi posiadać program do administrowania system telefonicznym
Wymagania systemu	Musi zapewnić automatyczny restart, samoczynne testowanie i automatyczne uruchamianie po włączeniu zasilania lub restarcie manualnym i powrót do normalnej pracy bez konieczności wykonywania dodatkowych czynności przez obsługę
Wymagania systemu	Redundantne zasilanie sieciowe gwarantujące bezprzerwową pracę systemu telefonicznego z wszystkimi elementami (min. dwa niezależne zasilacze sieciowe tzw. Hot Swap, pracujące w trybie gorącej rezerwy, w przypadku awarii jednego z zasilaczy drugi przejmuje zasilanie całego systemu)
Wymagania systemu	Musi posiadać możliwość rozszerzenia o aplikacje UC (Unified Communication) tego samego producenta w ramach pojedynczej jednostki sterującej, bez instalowania zewnętrznych urządzeń
Wymagania systemu	Musi posiadać możliwość uruchomienia zintegrowanego serwera faksów tego samego producenta, w ramach pojedynczej jednostki sterującej, bez instalowania zewnętrznych urządzeń
Wymagania systemu	Musi posiadać możliwość rozszerzenia o system DECT lub IP-DECT tego samego producenta, stacje bazowe powinny obsługiwać przynajmniej 12 jednoczesnych połączeń
Wymagania systemu	Możliwość rozbudowy o minimum 100 numerów wewnętrznych, tylko poprzez dołożenie kart rozszerzeń
Wymagania systemu	Możliwość rozszerzenia o aparaty systemowe IP tego samego producenta co system telefoniczny
Wymagania systemu	System musi zapewnić rozbudowę do co najmniej 500 użytkowników.
Wymagania systemu	Możliwość rozbudowy o łączność bezprzewodową w standardzie DECT/GAP oraz WLAN IP DECT - realizacja tylko poprzez dołożenie odpowiednich kart wewnętrznych do systemu, a przenośne aparaty DECT/IP DECT powinny realizować wszystkie funkcje stacjonarnego aparatu cyfrowego – systemowego
Wymagania systemu	Funkcja abonenta mobilnego (aparat GSM i/lub stacjonarny) powinien być dostępny jako numer wewnętrzny, mieć możliwość zalogowania się w centrali PBX i podlegać kategoriom aparatu wewnętrznego (możliwość wyjścia na zewnątrz jako numer wewnętrzny, przełączanie rozmowy, zestawiać telekonferencje, zapytania), mieć możliwość pracy równoległej z aparatem stacjonarnym (dzwonią jednocześnie stacjonarny aparat wewnętrzny i aparat mobilny sieci GSM)
Wymagania systemu	Możliwość dodania dwóch stanowisk fax-serwerów do obsługi funkcjonalności faksów
Zakres instalacji systemu	Ustalenie harmonogramu wykonywania prac z wskazanymi przez Zamawiającego osobami.
Zakres instalacji systemu	Prace wykonywane muszą być poza godzinami pracy Zamawiającego.

Zakres instalacji systemu	Montaż dostarczonego systemu telefonicznego ze wszystkimi elementami, zaprogramowanie zgodnie z możliwościami systemu i wymaganiami Zamawiającego
Zakres instalacji systemu	Szkolenie techniczne z administracji systemem telefonicznym
Zakres instalacji systemu	Szkolenie użytkowników aparatów systemowych z obsługi
Zakres instalacji systemu	Wykonanie dokumentacji powykonawczej zawierającej minimum: opis systemu, opis przełącznicy, certyfikaty i deklaracje dopuszczające do eksploatacji, dokumenty producenta (karty katalogowe, instrukcje), umożliwiające sprawdzenie oferowanych cech
Zakres instalacji systemu	Dostawa min. 20 tel. Wifi zgodnych z systemem telefonii

iii. archiwizacja danych (SW 5.4.I.2.3);

Biblioteka LTO – 1 szt.

Dla potrzeb projektu Wykonawca dostarczy bibliotekę taśmową z jednym napędem LTO6 z interfejsem SAS. Biblioteka będzie podłączona do serwera kopii zapasowych, czyli serwera backupu z wykorzystaniem interfejsu SAS.

- Montaż w szafie RACK 19". Maksymalnie 1U
- Ilość stacji LTO: 1
- Rodzaj napędu: LTO6
- Obsługiwane standardy kartridży:
 - LTO Ultrium 4
 - LTO Ultrium 5
 - LTO Ultrium 6
- Interfejs SAS 6 Gb/s
- Ilość obsługiwanych kartridży: 9
- Współczynnik kompresji danych: 2,5:1
- Maksymalna pojemność bez kompresji: 22,5 TB
- Maksymalna pojemność z kompresją: 56,25 TB
- Współczynnik transmisji bez kompresji: 160MB/s
- Współczynnik transmisji z kompresją: 400 MB/s
- Wbudowany skaner kodów kreskowych
- Interfejs zarządzający Ethernet
- Wbudowany frontowy panel zarządzający;
- Zarządzanie poprzez przeglądarkę WWW;
- Temperatura pracy: 10 – 40 °C
- Oprogramowanie do backupu danych

Oprogramowanie do archiwizacji danych

Nazwa komponentu	Wymagane minimalne parametry techniczne
	<p>Licencje muszą umożliwiać backup maszyn wirtualnych na serwerach fizycznych o łącznej liczbie 6 procesorów fizycznych. Licencja przeznaczona dla wykorzystywanego przez Wykonawcę środowiska wirtualizacji.</p> <p>Wszystkie licencje powinny być dostarczone wraz z 5-letnim wsparciem, świadczonym przez producenta oprogramowania, które powinno umożliwiać zgłaszanie problemów 5 dni w tygodniu przez 8h na dobę.</p>
	<ul style="list-style-type: none"> Oprogramowanie powinno współpracować z infrastrukturą VMware w wersji 4.0, 4.1, 5.0, 5.1, 5.5, 6 oraz Microsoft Hyper-V 2008 R2 SP1, 2012 I 2012 R2 Oprogramowanie powinno współpracować z hostami zarządzanymi przez VMware vCenter oraz Microsoft Virtual Machine Manager oraz z hostami niezarządzanymi Oprogramowanie powinno zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V
	<ul style="list-style-type: none"> Oprogramowanie powinno być licencjonowanie w modelu "per-CPU". Oprogramowanie powinno być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej Oprogramowanie powinno tworzyć "samowystarczalne" archiwa to odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków Oprogramowanie powinno mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej Oprogramowanie powinno zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia Oprogramowanie powinno zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP Oprogramowanie powinno mieć możliwość uruchamiania skryptów przed i po zadaniu backupowym Oprogramowanie powinno mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji Oprogramowanie powinno mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Oprogramowanie powinno wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
	<ul style="list-style-type: none"> Oprogramowanie powinno oferować podobne rozwiązanie jak CBT również dla platformy Hyper-V Oprogramowanie powinno wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn Oprogramowanie powinno mieć możliwość wydzielenia osobnej roli typu tape server Oprogramowanie powinno mieć możliwość kopiowania backupów do lokalizacji zdalnej Oprogramowanie powinno mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) Oprogramowanie powinno mieć możliwość replikacji wirtualnych maszyn pomiędzy lokalizacjami <p>Funkcjonalność ta powinna być zapewniona dla wirtualizatora</p>

- Oprogramowanie powinno dawać możliwość użycia wcześniej wykonanego backupu jako źródła do zadania replikacji
 - Oprogramowanie powinno wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
 - Oprogramowanie powinno dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego
 - Oprogramowanie powinno przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing)
- Oprogramowanie powinno umożliwić uruchomienie maszyny wirtualnej bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, bez potrzeby kopiowania jej na storage produkcyjny. Dla środowiska vSphere powinien być wykorzystany wbudowany w oprogramowanie serwer NFS. Dla Hyper-V powinna być zapewniona taka sama funkcjonalność realizowana wewnętrznymi mechanizmami oprogramowania
 - Oprogramowanie powinno umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
 - Oprogramowanie powinno umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny
 - Oprogramowanie powinno mieć możliwość odtworzenia plików przy pomocy VMware VIX API
 - Oprogramowanie powinno wspierać odtwarzanie plików z następujących systemów plików:
 - **Linux**
 - ext, ext2, ext3, ext4, ReiserFS (Reiser3), JFS, XFS
 - **Windows**
 - NTFS, FAT, FAT32, ReFS
 - Oprogramowanie powinno umożliwiać szybkie granularne odtwarzanie obiektów aplikacji takich jak Active Directory (dowolny obiekt, atrybut w tym hasło), Microsoft Exchange 2010 i nowsze (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"), Microsoft SQL 2005 i nowsze (w tym odtwarzanie point-in-time) oraz Microsoft Sharepoint 2010 i nowsze. Odtworzenie powinno być możliwe na serwery produkcyjne.
 - Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny.
 - Oprogramowanie powinno indeksować pliki Windows i Linux w celu szybkiego wyszukiwania
 - Oprogramowanie powinno używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows
 - Oprogramowanie powinno wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
- Oprogramowanie powinno dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V
 - Oprogramowanie powinno umożliwiać weryfikację odtwarzalności dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie.
 - Oprogramowanie powinno mieć podobne mechanizmy dla replik w środowisku vSphere.

Zamawiający posiada i użytkuje oprogramowanie Eset ERA. W celu zabezpieczenia sieci firmowej przed złośliwymi wirusami, wymaga się wdrożenia pakietu ochrony na 3 lat zawierającego:

- Ochronę komputerów licencja na 15 PC i 2 laptopy
 - Antywirus i antyspyware - Wbudowana ochrona dostępu do danych oraz zabezpieczenie przed wszystkimi rodzajami zagrożeń, m.in. przed wirusami, rootkitami, robakami i oprogramowaniem szpiegującym.
 - Kontrola urządzeń - Blokuje nieautoryzowane nośniki danych i urządzenia. Pozwala tworzyć reguły dla konkretnych typów, modeli i numerów seryjnych urządzeń oraz dla użytkowników.
 - Antyphishing - Chroni użytkowników przed stronami internetowymi, które podszywając się pod zaufane serwisy WWW, próbują zdobyć poufne informacje - nazwy użytkowników, hasła, dane kart kredytowych.
 - Blokada programów typu exploit - Nowa technologia wykrywania złośliwych programów, która eliminuje zagrożenia blokujące komputer i wyłudzające okup. Chroni przed atakami, wykorzystującymi luki w przeglądarkach internetowych, czytnikach PDF, czy oprogramowaniu Java.
 - Zaawansowany skaner pamięci - Rozbudowuje dotychczasową ochronę antywirusową o skuteczne zabezpieczenie przed skomplikowanymi zagrożeniami, wielokrotnie spakowanymi lub zaszyfrowanymi.
- Ochronę serwerów plikowych licencja na 2 serwery
 - Zoptymalizowany dla środowiska wirtualnego
 - Pełne wsparcie dla środowisk klastrowych
 - Skanowanie przechowywanych plików
 - Wyszczególnione narzędzie czyszczące
- Centralne zarządzanie
 - Wsparcie dla wielu platform - Działa na systemach Windows i Linux.
 - Webowa konsola
 - License Administrator - Pozwala w łatwy i przejrzysty sposób zarządzać w czasie rzeczywistym z jednego miejsca wszystkimi licencjami - wszystko za pośrednictwem przeglądarki internetowej.
 - Zdalna instalacja na stacjach roboczych
 - Polityki bezpieczeństwa - Pozwala na wdrożenie danej polityki bezpośrednio na agencie. Pozwala stosować określone polityki dla grup dynamicznych.
 - Raportowanie - zbiera tylko niezbędne dane do raportów, przechowując logi na kliencie, co skutkuje lepszą wydajnością bazy danych.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Ogólne	1. Pełne wsparcie dla systemu Windows XP SP3/Vista/Windows 7/Windows8/Windows 8.1/Windows 8.1 Update/10 2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows. 3. Wersja programu dla stacji roboczych Windows dostępna zarówno w języku polskim jak i angielskim.

	<ol style="list-style-type: none"> Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim. Skuteczność programu potwierdzona nagrodami VB100 i AV-comparatives
Ochrona antywirusowa i antyspyware	<ol style="list-style-type: none"> Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. Wbudowana technologia do ochrony przed rootkitami. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania). Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. Możliwość skanowania dysków sieciowych i dysków przenośnych. Skanowanie plików spakowanych i skompresowanych. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.

18. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
19. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
20. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego).
21. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
22. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
23. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
24. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
25. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
26. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony.
27. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora.
28. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
29. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
30. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
31. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta.
32. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.

33. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
34. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.
35. Użytkownik musi posiadać możliwość przestania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
36. W przypadku gdy stacja robocza nie będzie posiadała dostępu do sieci Internet ma odbywać się skanowanie wszystkich procesów również tych, które wcześniej zostały uznane za bezpieczne.
37. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
38. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń mają być wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
39. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.
40. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
41. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
42. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
43. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.
44. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.
45. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.

46. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji.
47. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykłe oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
48. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.
49. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
50. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
51. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM , urządzeń przenośnych oraz urządzeń dowolnego typu.
52. Funkcja blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model.
53. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia, dana funkcjonalność musi pozwalać na automatyczne wypełnienie właściwości urządzenia dla tworzonej reguły.
54. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie brak dostępu do podłączanego urządzenia.
55. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
56. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.

57. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika
58. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
59. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
 - tryb automatyczny z regułami gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
 - tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
 - tryb oparty na regułach gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
 - tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach.
 - Tryb inteligentny – w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.
60. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
61. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
62. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
63. Program musi być wyposażona w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp.
64. Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.
65. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.
66. Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
67. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.

68. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.
69. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur.
70. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.
71. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http
72. Program musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback).
73. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapor sieciowa).
74. Program ma być w pełni zgodny z technologią CISCO Network Access Control.
75. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym.
76. W momencie wykrycia trybu pełno ekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji.
77. Użytkownik ma mieć możliwość skonfigurowania programu tak aby automatycznie program włączał powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym po określonym przez użytkownika czasie.
78. Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania.
79. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
80. Program musi posiadać możliwość utworzenia z poziomu interfejsu aplikacji dziennika diagnostycznego na potrzeby pomocy technicznej.
81. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline.
82. Możliwość podejrzenia licencji za pomocą, której program został aktywowany.

	83. W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: ochrona antywirusowa i antyspyware, kontrola dostępu do urządzeń, zaporą osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, , Obsługa technologii Microsoft NAP.
Ochrona przed spamem	<ol style="list-style-type: none"> 1. Ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail. 2. Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej. 3. Pełna integracja z programami pocztowymi MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail – antyspamowe funkcje programu dostępne są bezpośrednio z paska menu programu pocztowego. 4. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego. 5. Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną wiadomość i odwrotnie oraz ręcznego dodania wiadomości do białej i czarnej listy z wykorzystaniem funkcji programu zintegrowanych z programem pocztowym. 6. Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam. 7. Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam. 8. Program ma umożliwiać współpracę w swojej domyślnej konfiguracji z folderem „Wiadomości śmieci” obecnym w programie Microsoft Outlook. 9. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną zmieni jej właściwość jako „nieprzeczytana” oraz w momencie zaklasyfikowania wiadomości jako spam na automatyczne ustawienie jej właściwości jako „przeczytana”. 10. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.
Zapora osobista	<ol style="list-style-type: none"> 1. Zapora osobista ma pracować jednym z 4 trybów: <ul style="list-style-type: none"> • tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące, jednocześnie umożliwia utworzenie dodatkowych reguł przez administratora • tryb interaktywny – program pyta się o każde nowe nawiązywane połączenie i automatycznie tworzy dla niego regułę (na stałe lub tymczasowo), • tryb oparty na regułach – użytkownik/administrator musi ręcznie zdefiniować reguły określające jaki ruch jest blokowany a jaki przepuszczany,

	<ul style="list-style-type: none"> • tryb uczenia się – umożliwia zdefiniowanie przez administratora określonego okresu czasu w którym oprogramowanie samo tworzy odpowiednie reguły zapory analizując aktywność sieciową danej stacji. <ol style="list-style-type: none"> 2. Możliwość tworzenia list sieci zaufanych. 3. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie 4. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego. 5. Możliwość wyboru jednej z 3 akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj o decyzję. 6. Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń. 7. Możliwość zapisywania w dzienniku zdarzeń związanych z zezwoleniem lub zablokowaniem danego typu ruchu. 8. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet. 9. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 10. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet. 11. Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu. 12. Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6. 13. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci. 14. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci 15. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora. 16. Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowaniu sieci bezprzewodowej lub jego braku, aktywności połączenia bezprzewodowego lub jego braku, konkretny interfejs sieciowy w systemie. 17. Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS zarówno z wykorzystaniem adresów IPv4 jak i IPv6 18. Opcje związane z autoryzacją stref mają oferować opcje łączenia (np. lokalny adres IP i adres serwera DNS) w dowolnej kombinacji celem zwiększenia dokładności identyfikacji danej sieci.
--	---

	<p>19. Program musi umożliwić ustalenie tymczasowej czarnej listy adresów IP, które będą blokowane podczas próby połączenia.</p> <p>20. Program musi posiadać kreator, który umożliwia rozwiązać problemy z połączeniem. Musi on działać w oparciu o:</p> <ul style="list-style-type: none"> rozwiązanie problemów z aplikacją lokalną którą wskazujemy z listy. Dana reguła będzie mogła obowiązywać przez określony okres czasu. <p>11. rozwiązywanie problemów z połączeniem z urządzeniem zdalnym na podstawie adresu IP, dana reguła będzie mogła obowiązywać przez określony okres czasu.</p>
Kontrola dostępu do stron internetowych	<ol style="list-style-type: none"> Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły. Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego. Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika. Aplikacja musi posiadać możliwość filtrowania url w oparciu o co najmniej 140 kategorii i pod kategorii. Podstawowe kategorie w jakie aplikacja musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii. Moduł musi posiadać także możliwość grupowania kategorii już istniejących. Lista adresów url znajdujących się w poszczególnych kategoriach musi być na bieżąco aktualizowana przez producenta. Użytkownik musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych. Aplikacja musi posiadać możliwość określenia uprawnień dla dostępu do kategorii url – zezwól, zezwól i ostrzeż, blokuj. Program musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania określonej w regułach witryny.
Ochrona serwera plików	<ol style="list-style-type: none"> Wsparcie dla systemów: Microsoft Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2, 2016, SBS 2003, SBS 2003 R2, SBS 2008, SBS 2011, Microsoft MultiPoint Server 2010, Microsoft MultiPoint Server 2011, Windows MultiPoint Server 2012.

2. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
4. Wbudowana technologia do ochrony przed rootkitami i exploitami.
5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
7. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
8. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
9. System antywirusowy ma mieć możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
10. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.
11. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego.
12. Możliwość skanowania dysków sieciowych i dysków przenośnych.
13. Skanowanie plików spakowanych i skompresowanych.
14. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
15. Program musi posiadać funkcjonalność pozwalającą na ograniczenie wielokrotnego skanowania plików w środowisku wirtualnym za pomocą mechanizmu przechowywującego informacje o przeskanowanym już obiekcie i współdzieleniu tych informacji z innymi maszynami wirtualnymi.
16. Aplikacja powinna wspierać mechanizm klastrowania.
17. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
18. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS.
19. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.

20. Program ma umożliwiać użytkownikowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, płyt CD/DVD i pamięci masowych FireWire.
21. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia.
22. Aplikacja musi posiadać funkcjonalność, która automatycznie uzupełni elementy wymagane dla tworzenia reguł w oparciu o informacje dostępne z aktualnie podłączonego nośnika.
23. Aplikacja ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, brak dostępu do podłączanego urządzenia.
24. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
25. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
26. System antywirusowy ma automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
27. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
28. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.
29. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
30. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.
31. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione.
32. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.
33. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).
34. Możliwość przeniesienia zainfekowanych plików w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.

35. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
36. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.
37. Aktualizacje modułów analizy heurystycznej.
38. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
39. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
40. Wysyłanie zagrożeń do laboratorium ma być możliwe z serwera zdalnego zarządzania i lokalnie z każdej stacji roboczej w przypadku komputerów mobilnych.
41. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
42. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
43. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.
44. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła.
45. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło.
46. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo.

47. System antywirusowy ma być w pełni zgodny z technologią CISCO NAC.
48. System antywirusowy ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.
49. System antywirusowy ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykłe oraz aktualizacje o niskim priorytecie. Program ma także posiadać opcję dezaktywacji tego mechanizmu.
50. Po instalacji systemu antywirusowego, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.
51. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
52. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
53. Program powinien umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: nośników CD/DVD oraz urządzeń USB.
54. System antywirusowy ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.
55. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.
56. System antywirusowy ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
57. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
58. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy

	<p>pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).</p> <p>59. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.</p> <p>60. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja).</p> <p>61. Do każdego zadania aktualizacji można przypisać dwa różne profile z innym ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja). Przykładowo, domyślny profil aktualizuje z sieci lokalnej a w przypadku jego niedostępności wybierany jest profil rezerwowy pobierający aktualizację z Internetu.</p> <p>62. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).</p> <p>63. Aplikacja musi wspierać skanowanie magazynu Hyper-V</p> <p>64. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów</p> <p>65. Praca programu musi być niezauważalna dla użytkownika.</p> <p>66. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania.</p> <p>67. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.</p>
Administracja zdalna	<ol style="list-style-type: none"> 1. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2003, 2008, 2012 oraz systemach Linux. 2. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance). 3. Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL. 4. Serwer administracyjny musi oferować możliwość wykorzystania już istniejącej bazy danych MS SQL lub MySQL użytkownika. 5. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów oddzielnie bezpośrednio ze strony producenta.

6. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej.
7. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy występujące w sieci.
8. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6.
9. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający.
10. Zmiana języka panelu administracyjnego nie może wymagać zatrzymania lub reinstalacji oprogramowania zarządzającego.
11. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL.
12. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
13. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
14. Jeden centralny serwer centralnego zarządzania bez względu na wielkość sieci.
15. Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci – serwer pośredniczący (proxy) lub serwer centralny.
16. Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym.
17. Serwer proxy musi być wyposażony we własną bazę danych, w której będą przechowywane dane z agentów na wypadek braku połączenia z serwerem centralnym.
18. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.
19. Serwer administracyjny musi oferować możliwość instalacji serwera http proxy pozwalającego na pobieranie aktualizacji baz sygnatur oraz pakietów instalacyjnych na stacjach roboczych bez dostępu do Internetu.
20. Serwer http proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) najczęściej pobieranych elementów.
21. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
22. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.

23. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na stacjach roboczych z systemami Windows, Mac OS X oraz Linux oraz serwerach Windows.
24. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na urządzeniach mobilnych z systemem Android.
25. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.
26. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
27. Administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami nie posiadającymi zainstalowanego programu zabezpieczającego.
28. Agent musi przekazywać informacje na temat stanu systemu operacyjnego do serwera administracji zdalnej.
29. Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania.
30. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
31. Instalacja agenta musi odbywać się przy wykorzystaniu repozytorium producenta. Repozytorium powinno zawierać aktualne wersje agentów bez względu na rodzaj systemu operacyjnego.
32. Instalacja agenta nie może wymagać określenia typu systemu (32 lub 64 – bitowy) oraz jego rodzaju (Windows, Mac, itp) a dobór odpowiedniego pakietu musi być w pełni automatyczny.
33. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika.
34. W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play.
35. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.
36. Serwer administracyjny musi oferować możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym

- urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, nie komunikację za pośrednictwem wiadomości SMS.
37. Serwer administracyjny musi oferować możliwość utworzenia polityk konfiguracji dla aplikacji zabezpieczającej na urządzeniu mobilnym.
 38. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi.
 39. Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej
 40. Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji.
 41. Administrator musi posiadać możliwość utworzenia użytkownika wbudowanego lub zintegrowanego z grupą z usługi Active Directory.
 42. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp.
 43. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis.
 44. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
 45. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta bez konieczności logowania się do panelu administracyjnego.
 46. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany.
 47. Dostępne zadania muszą być podzielone na dwie grupy: zadania klienta oraz zadania serwera.
 48. Zadania serwera obejmujące zadanie instalacji agenta, generowania raportów oraz synchronizacji grup.
 49. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.
 50. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.

51. Serwer administracyjny musi w przejrzysty sposób informować administratora o elementach zadań jakie są wymagane do jego uruchomienia a w przypadku jego braku wskazywać brakujące elementy konfiguracji.
52. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym.
53. Serwer administracyjny musi oferować możliwość wyboru parametrów pakietu instalacyjnego zależnych od systemu operacyjnego oraz licencji na program zabezpieczający.
54. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu.
55. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stację kliencką.
56. Serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy.
57. Serwer administracyjny musi oferować możliwość uruchomienia zadania automatycznie zgodnie z harmonogramem, po wystąpieniu nowego dziennika zdarzeń lub umieszczeniu nowego klienta w grupie dynamicznej.
58. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów.
59. Grupy dynamiczne tworzone na podstawie szablonu określającego warunki jakie musi spełnić klient aby zostać umieszczony w danej grupie. Przykładowe warunki: Adresy sieciowe IP, Aktywne zagrożenia, Stan funkcjonowania/ochrony, Wersja systemu operacyjnego, itp.
60. Serwer administracyjny musi oferować możliwość utworzenia polityk dla programów zabezpieczających i modułów serwera centralnego zarządzania.
61. Serwer administracyjny musi oferować możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. Serwer administracyjny musi oferować możliwość przypisania kilku polityk z innymi priorytetami dla jednego klienta.
62. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej.
63. Serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś” dla konkretnej opcji w konfiguracji klienta. Opcja ta nie będzie mogła być zmieniona na stacji klienckiej bez

	<p>względem na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku.</p> <p>64. Serwer administracyjny musi oferować możliwość ukrycia graficznego interfejsu użytkownika na stacji klienckiej i jego uruchomienia tylko przez administratora.</p> <p>65. Serwer administracyjny musi umożliwiać wyświetlenie polityk do których przynależy dana stacja robocza oraz ich edycję z poziomu właściwości samego klienta</p> <p>66. Serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów.</p> <p>67. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania.</p> <p>68. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie.</p> <p>69. Serwer administracyjny musi oferować możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy, itp.</p> <p>70. Serwer administracyjny musi oferować możliwość określenia danych jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na elementach wykresu oraz ich odfiltrowania i posortowania.</p> <p>71. Serwer administracyjny musi być wyposażona w mechanizm importu oraz eksportu szablonów raportów.</p> <p>72. Serwer administracyjny powinien posiadać Panel kontrolny z raportami administratora, pozwalający na szybki dostęp do najbardziej interesujących go danych. Panel ten musi oferować możliwość modyfikacji jego elementów.</p> <p>73. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW.</p> <p>74. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS.</p> <p>75. Serwer administracyjny musi oferować możliwość skonfigurowania czasu automatycznego odświeżania raportu na panelu kontrolnym oraz umożliwiać jego odświeżenie na żądanie.</p>
--	---

76. Serwer administracyjny musi oferować możliwość tworzenia wielu zakładek panelu, w których będą widoczne wybrane przez administratora elementy monitorujące.
77. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego.
78. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
79. Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień lub skorzystanie z predefiniowanych wzorów.
80. Powiadomienia muszą dotyczyć zmiany ilości klientów danej grupy dynamicznej, wzrostu liczby grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń lub skanowania lub stanu obiektu serwer centralnego zarządzania.
81. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP.
82. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu.
83. Serwer administracyjny musi oferować możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.
84. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta.
85. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji.
86. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty.
87. Serwer administracyjny musi oferować możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.
88. Narzędzie administracyjne musi być wyposażone w mechanizm wyszukiwania zarządzanych komputerów na podstawie co najmniej nazwy komputera, adresu IPv4 i IPv6 lub wyszukiwania konkretnej nazwy zagrożenia.
89. Serwer administracyjny musi być wyposażona w mechanizm autodopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana.

	90. Administrator musi mieć możliwość określenia zakresu czasu w jakim dane zadanie będzie wykonywane (sekundy, minuty, godziny, dni, tygodnie).
--	--

v. zapewnienie ciągłości pracy systemu (SW 5.4.1.2.5);

Zapewnienie ciągłości pracy systemów musi zostać oparte o wirtualizację systemów operacyjnych. W tym celu Wykonawca jest zobowiązany do upgrade oprogramowania wirtualizacyjnego używanego przez Zamawiającego VMware ESX Essential oraz objęciem wirtualizacją 4 serwerów zamawianych w niniejszym zamówieniu tak aby stworzyć jednorodne środowisko na wszystkich serwerach zamawiającego według poniższych wymagań.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Oprogramowanie do wirtualizacji	<p>Licencje muszą umożliwiać uruchamianie wirtualizacji na oferowanych serwerach fizycznych oraz jednej konsoli do zarządzania całym środowiskiem.</p> <p>Wszystkie licencje powinny być dostarczone wraz z 5-letnim wsparciem, świadczonym przez producenta będącego licencjodawcą oprogramowania na pierwszym, drugim i trzecim poziomie, które powinno umożliwiać zgłaszanie problemów 5 dni w tygodniu przez 8h na dobę.</p>
Konsolidacja	<ul style="list-style-type: none"> Warstwa wirtualizacji musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym i nie może być częścią innego systemu operacyjnego. Warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 200MB pamięci operacyjnej RAM serwera fizycznego. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym. Wymagana jest możliwość przydzielenia maszynie większej ilości wirtualnej pamięci operacyjnej niż jest zainstalowana w serwerze fizycznym oraz większej ilości przestrzeni dyskowej niż jest fizycznie dostępna. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością dostępu do 4TB pamięci operacyjnej. Oprogramowanie do wirtualizacji musi zapewnić możliwość przydzielenia maszynom wirtualnym do 128 procesorów wirtualnych. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. Rozwiązanie musi w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.

- Rozwiązanie musi wspierać następujące systemy operacyjne: Windows XP, Windows Vista, Windows NT, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012R2, SLES 11, SLES 10, SLES9, SLES8, Ubuntu 7.04, RHEL 5, RHEL 4, RHEL3, RHEL 2.1, Solaris wersja 10 dla platformy x86, NetWare 6.5, NetWare 6.0, NetWare 6.1, Debian, CentOS, FreeBSD, Asianux, Ubuntu 7.04, SCO OpenServer, SCO Unixware, Mac OS X.
- 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 2012/2012R2 na maszynie wirtualnej.
- Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania środowiskiem serwerów wirtualnych. Konsola graficzna musi być dostępna poprzez dedykowanego klienta i za pomocą przeglądarek, minimum IE i Firefox.
- Dostęp przez przeglądarkę do konsoli graficznej musi być skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska.
- Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta root.
- Rozwiązanie musi umożliwiać składowanie logów ze wszystkich serwerów fizycznych i konsoli zarządzającej na serwerze Syslog. Serwer Syslog w dowolnej implementacji musi stanowić integralną część rozwiązania.
- Rozwiązanie musi zapewnić możliwość monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej i zdefiniowania alertów informujących o przekroczeniu wartości progowych.
- Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji.
- Rozwiązanie musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi.
- Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii zapasowych instancji systemów operacyjnych oraz ich odtworzenia w możliwie najkrótszym czasie.
- Kopie zapasowe muszą być składowane z wykorzystaniem technik de-duplikacji danych.
- Musi istnieć możliwość odtworzenia pojedynczych plików z kopii zapasowej maszyny wirtualnej przez osoby do tego upoważnione

	<p>bez konieczności nadawania takim osobom bezpośredniego dostępu do głównej konsoli zarządzającej całym środowiskiem.</p> <ul style="list-style-type: none"> • Mechanizm zapewniający kopie zapasowe musi być wyposażony w system cyklicznej kontroli integralności danych. Ponadto musi istnieć możliwość przywrócenia stanu repozytorium kopii zapasowych do punktu w czasie, kiedy wszystkie dane były integralne w przypadku jego awarii. • Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością wskazania konieczności zachowania stanu pamięci pracującej maszyny wirtualnej. • Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi. • Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności: Microsoft Active Directory, Open LDAP. • Platforma wirtualizacyjna musi umożliwiać zastosowanie w serwerach fizycznych procesorów o dowolnej ilości rdzeni. • Rozwiązanie musi umożliwiać tworzenie jednorodnych wolumenów logicznych o wielkości do 62TB. • Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie przestrzeni dyskowej. • Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej. • Rozwiązanie musi umożliwiać wykorzystanie technologii 10GbE w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi. • Rozwiązanie musi zapewniać możliwość replikacji maszyn wirtualnych z dowolnej pamięci masowej w tym z dysków wewnętrznych serwerów fizycznych na dowolną pamięć masową w tym samym lub oddalonym ośrodku przetwarzania. • Rozwiązanie musi gwarantować współczynnik RPO na poziomie minimum 5 minut • Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum. • Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.
--	---

	<ul style="list-style-type: none"> Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek. System musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowane wirtualne urządzenia dedykowane dla poszczególnych maszyn wirtualnych.
Wysoka dostępność	<ul style="list-style-type: none"> Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi, niezależnie od dostępności współdzielonej przestrzeni dyskowej, różnymi rodzajami wirtualnych przełączników sieciowych. Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały automatycznie przełączone na inne serwery infrastruktury. Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury. Rozwiązanie musi zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania. Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej wliczając w to zarówno poprawki bezpieczeństwa jak i zmianę jej wersji. 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. 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.
Równoważenie obciążenia i przestoje serwisowe	<ul style="list-style-type: none"> Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum. Konieczna jest możliwość przenoszenia usług pomiędzy serwerami fizycznymi, bez przerywania pracy usług. System musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu do pamięci masowych oraz ustalania priorytetów dostępu do nich na poziomie konkretnych wirtualnych maszyn.

vi. uwierzytelnianie i autoryzacja użytkowników systemu (SW 5.4.I.2.6);

Użytkownicy systemu będą uwierzytelniani w systemie za pomocą systemów SSO opartych o katalog użytkowników LDAP opartych o struktury domeny. Użytkownicy zewnętrzni zostaną uwierzytelniani za pomocą odrębnej bazy danych użytkowników e-Usług. System ten zostanie opisany przy okazji opisu przedmiotu zamówienia dla e-Usług.

Minimalne wymagania dla serwerowych systemów operacyjnych

Nazwa komponentu	Wymagane minimalne parametry techniczne
Wykonawca dostarczy odpowiednią liczbę licencji zgodną z ilością serwerów i zainstalowanych w nich procesorów oraz licencje dostępowe w ilości zgodnej z opisem przy serwerach.	
Licencje mają uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w oferowanym środowisku FT na minimum 12 maszynach wirtualnych.	
Serwerowy system operacyjny (dalej: SSO) posiada następujące, wbudowane cechy.	
1	Posiada możliwość wykorzystania 320 logicznych procesorów oraz 4 TB pamięci RAM w środowisku fizycznym
2	Posiada możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności 64TB przez każdy wirtualny serwerowy system operacyjny.
3	Posiada możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych.
4	Posiada możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5	Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6	Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7	Posiada automatyczną weryfikację cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8	Posiada możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten uwzględnia specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9	Wbudowane wsparcie instalacji i pracy na wolumenach, które: <ul style="list-style-type: none"> – pozwalają na zmianę rozmiaru w czasie pracy systemu, – umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, – umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10	Posiada wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.

11	Posiada wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12	Posiada możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13	Posiada możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14	Posiada wbudowaną zaporę internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15	Graficzny interfejs użytkownika.
16	Zlokalizowane w języku polskim, następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
17	Posiada wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
18	Posiada możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
19	Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
20	Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).
21	Posiada możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
22	Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
23	<p>Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:</p> <ul style="list-style-type: none"> – Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, – Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, – Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. – Zdalna dystrybucja oprogramowania na stacje robocze. – Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej – Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: <p>Dystrybucję certyfikatów poprzez http Konsolidację CA dla wielu lasów domeny, Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen. Szyfrowanie plików i folderów. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).</p>

	<ul style="list-style-type: none"> – Posiada możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów. – Serwis udostępniania stron WWW. – Wsparcie dla protokołu IP w wersji 6 (IPv6), – Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, – Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji zapewniają wsparcie dla: Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, Obsługi ramek typu jumbo frames dla maszyn wirtualnych. Obsługi 4-KB sektorów dysków Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra. – Posiada możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. – Posiada możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model) <p>Posiada możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.</p>
24	Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
25	Posiada możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
26	Posiada mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
27	Posiada możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

vii. zarządzanie zasobami systemu informatycznego (SW 5.4.1.2.7);

Wszystkie systemy środowiska serwerowego wymienionego w HRF II.4.a muszą być zarządzane z jednej konsoli systemowej. Zamawiający obecnie używa konsolę systemową dla infrastruktury zwirtualizowanej vCenter. Wykonawca musi wyposażyć swoją instalację w system mogący zarządzać infrastrukturą serwerową obecną i docelową (lub je wymienić) z jednego miejsca, tak aby nie duplikować

systemów zarządzania. Dodatkowo Wykonawca musi wdrożyć infrastrukturę LDAP lub rozszerzyć o serwery wdrażane obecnie funkcjonującą infrastrukturę Active Directory.

viii. oprogramowanie do zarządzania i monitorowania infrastruktury technicznej (SW 5.4.I.2.8).

Wykonawca w ramach zamówienia musi wdrożyć system zarządzania i monitoringu pracy środowiska serwerowni. Zakres monitoringu zostanie ustalony z Zamawiającym na etapie analizy przedwdrożeniowej. Wykonawca w celu wykonania zadania może użyć i dostosować oprogramowanie funkcjonujące już w infrastrukturze Zamawiającego Axence lub zastosować inne oprogramowanie.

Ad 2. Zakup sprzętu komputerowego (HRF II.2)

- a. modernizacja użytkowanego sprzętu komputerowego – komputery stacjonarne, przenośne, urządzenia drukujące, skanery, w tym zakup nowych jednostek sprzętu (SW 5.4.I.1.6);

1. Komputery stacjonarne (all in one) PC – 15 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Typ	Komputer stacjonarny. Typu All in One, komputer wbudowany w monitor.
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna
Wydajność	SYSmark® 2014 PerformanceTest : - SM 2014 Overall RRating – co najmniej wynik 1410 punktów, - Office Productivity – co najmniej wynik 1350 punktów, - Media Creation – co najmniej wynik 1400 punktów, - Data/Financial Analysis – co najmniej wynik 1470 punktów, Zamawiający zastrzega sobie możliwość wezwania Wykonawcy do przedstawienia próbki oferowanego komputera do przeprowadzenia testów wydajności.
Procesor	Procesor wielordzeniowy ze zintegrowaną grafiką, osiągający w teście PassMark CPU Mark wynik min. 5330 punktów
Pamięć operacyjna RAM	8GB DDR3 1600MHz non-ECC możliwość rozbudowy do min 16GB
Parametry pamięci masowej	Min. 240 GB SSD o prędkości zapisu/odczytu 500MB/s dla systemu operacyjnego lub pamięć PCI-Express
Wydajność grafiki	Grafika zintegrowana z procesorem powinna umożliwiać pracę dwumonitorową z wsparciem DirectX 11.1, OpenGL 4.0, OpenCL 1.2; pamięć współdzielona z pamięcią RAM, dynamicznie przydzielana do min. 1,7GB

	Oferowana karta graficzna musi osiągać w teście PassMark Performance Test co najmniej wynik 970 punktów w G3D Rating, wynik dostępny na stronie: http://www.videocardbenchmark.net/gpu_list.php	
Matryca	Rozmiar matrycy / plamki	min. 21,5" / max. 0,25mm
	Max. rozdzielczość	FHD (1920x1080)
	Jasność / kontrast	min. 250 cd/m ² / min. 600:1
	Głębokość koloru	16.7mln
	Czas odpowiedzi	max. 25 msec
	Odświeżanie	min. 60 Hz
Wypożyczenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, 24-bitowa konwersja sygnału cyfrowego na analogowy i analogowego na cyfrowy	
Obudowa	<p>Typu All-in-One zintegrowana z monitorem min. 21,5". Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) lub kłódki (oczko w obudowie do założenia kłódki),</p> <p>Demontaż standu musi odbywać się bez użycia narzędzi, mocowanie standu opatrzone w przycisk zwalniający.</p> <p>Demontaż tylnej pokrywy musi odbywać się bez użycia narzędzi, nie dopuszcza się stosowania śrub motylkowych, radełkowych czy zwykłych wkrętów. Suma wymiarów samej obudowy (bez podstawy) nie może przekraczać 99cm, Możliwość zainstalowania komputera na ścianie przy wykorzystaniu ściennego systemu montażowego VESA 100,</p> <p>Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszczonym na obudowie, oraz musi być wpisany na stałe w BIOS.</p> <p>Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń, napędu optycznego i dysku twardego bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych, śrub radełkowych).</p> <p>Obudowa musi posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzającym – diagnostycznym.</p> <p>Wbudowany wizualny system diagnostyczny włącznika POWER, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED przycisku POWER [tzn. barw i miganie] W szczególności musi sygnalizować:</p> <ul style="list-style-type: none"> - uszkodzenie lub brak pamięci RAM - uszkodzenie płyty głównej [w tym również portów I/O, chipset] - uszkodzenie kontrolera Video - awarię BIOS'u - awarię procesora 	

	<p>Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnek zewnętrznych w specyfikacji oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji, a które nie są dedykowane dla systemu diagnostycznego.</p> <p>Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszczonym na obudowie, oraz musi być wpisany na stałe w BIOS.</p>
Zgodność z systemami operacyjnymi i standardami	Potwierdzenie kompatybilności komputera na daną platformę systemową (wydruk ze strony)
Bezpieczeństwo	<p>Wbudowany, czyli wlutowany (nie dopuszcza się zintegrowanych z płytą główną tzn. układ wykorzystujący jakiegokolwiek złącza wyprowadzone na płycie) w płycie głównej dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej.</p> <p>Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot'owania, umożliwiający jednocześnie przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego.</p> <p>System opatrzony min. o funkcjonalność:</p> <ul style="list-style-type: none"> - sprawdzenie Master Boot Record na gotowość do uruchomienia oferowanego systemu operacyjnego, - test procesora [min. cache] - test pamięci, - test wentylatora dla procesora i dodatkowego wentylatora [w przypadku zamontowania] - test podłączonych kabli - test podłączonego wyświetlacza - test portów USB - test dysku twardego <p>Zasilacz wyposażony swój własny system diagnostyczny niezależny od pozostałych komponentów oferowanego komputera umożliwiający sprawdzenie poprawnego funkcjonowania zasilacza bez narażania pozostałych składowych na ewentualne uszkodzenia (przebiecia itp.)</p> <p>Czujnik otwarcia obudowy musi zbierać logi i zapisywać je w BIOS.</p> <p>Każdy komputer musi mieć min. 500VA UPS biurkowy.</p>
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość

	włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu).
BIOS	<p>BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera, Pełna obsługa BIOS za pomocą klawiatury i myszy.</p> <p>Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:</p> <ul style="list-style-type: none"> • wersji BIOS, • nr seryjnym komputera, • specjalny kod serwisowy • dacie wyprodukowania komputera, • dacie wysyłki komputera z fabryki, • włączonej lub wyłączonej funkcji aktualizacji BIOS • ilości zainstalowanej pamięci RAM, • ilości dostępnej pamięci RAM, [dostępna pamięć RAM po odjęciu obszaru pamięci RAM dla zintegrowanego układu graficznego w BIOS], • prędkości zainstalowanych pamięci RAM, • aktywnym kanale – dual channel, • technologii wykonania pamięci, • sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki : • DIIMM 1, DIMM 2, • typie zainstalowanego procesora, • ilości rdzeni zainstalowanego procesora, • numerze ID procesora nadawanego przez producenta procesora, • typowej prędkości zainstalowanego procesora • minimalnej osiąganey prędkości zainstalowanego procesora, • maksymalnej osiąganey prędkości zainstalowanego procesora, • pamięci cache L2 zainstalowanego procesora, • pamięci cache L3 zainstalowanego procesora, • czy zainstalowany procesor wykorzystuje technologię HT (wielowątkowość) • czy procesor jest wykonany w technologii 64-bit • zainstalowanych dyskach twardych • o wszystkich urządzeniach podpiętych na płycie głównej za pomocą złącza M.2 • rodzajach napędów optycznych • MAC adresie zintegrowanej karty sieciowej, • zintegrowanym układzie graficznym,

	<ul style="list-style-type: none"> • kontrolerze audio • Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS) • Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń. • Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na poziomie systemu, administratora oraz dysku twardego, • możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) oraz uprawniającego do samodzielnej zmiany tego hasła przez użytkownika (bez możliwości zmiany innych parametrów konfiguracji BIOS) przy jednoczesnym zdefiniowanym hasle administratora i/lub zdefiniowanym hasle dla dysku Twardego. Użytkownik po wpisaniu swojego hasła jest w stanie jedynie zmienić hasło dla dysku twardego. • Możliwość zdefiniowania mocy haseł do 32 znaków, • Możliwość wyłączenia/włączenia karty sieciowej, • Możliwość włączenia/wyłączenia kontrolera SATA • Możliwość włączenia/wyłączenia technologii raportowania i zgłaszania błędów zainstalowanego dysku twardego podczas uruchamiania systemu, technologia ta jest analizą samokontrolną, • Możliwość włączenia/wyłączenia kontrolera audio, • Możliwość włączenia/wyłączenia klawiszy OSD • Możliwość włączenia/wyłączenia dotyku ekranu (funkcja na stałe zaimplementowana w BIOS ale dostępna i aktywna tylko dla matrycy dotykowej) • Możliwość włączenia/wyłączenia wbudowanej kamery • Możliwość włączenia/wyłączenia czytnika kart multimedialnych • Możliwość włączenia/wyłączenia układu TPM. • Możliwość wyłączenia czujnika otwarcia obudowy, • Możliwość ustawienia czujnika obudowy w tryb cichy - nie informuje użytkownika o otwarciu obudowy (dźwiękiem i komunikatem) ale zapisuje log operacji. • Możliwość włączenia/wyłączenia funkcji ochrony dysku twardego [funkcja niezależna od TPM] • Możliwość ręcznego zdefiniowania zapotrzebowania na ilość rdzeni procesora dla aplikacji a w szczególności dla starszych, mających problemy z nowymi procesorami, • Możliwość ręcznego włączenia/wyłączenia funkcji, która pozwalająca na dynamiczną zmianę wartości mnożnika i
--	---

	<p>napięcia [funkcja związana z architekturą procesora, nie dopuszcza się overclockingu, zaimplementowana na stałe w BIOS ale aktywna przy procesorze w pełni wspierającym],</p> <ul style="list-style-type: none"> • Możliwość ręcznego włączenia/wyłączenia funkcji uśpienia procesora dla systemu operacyjnego w trybie bezczynności w celu zwiększenia oszczędności energii [funkcja zaimplementowana na stałe w BIOS ale aktywna przy procesorze w pełni wspierającym], • Możliwość ręcznego włączenia/wyłączenia funkcji procesora, która automatycznie zwiększa taktowanie procesora, gdy komputerowi potrzebna jest wyższa prędkość obliczeniowa [funkcja zaimplementowana na stałe w BIOS ale aktywna przy procesorze w pełni wspierającym], • Możliwość ręcznego włączenia/wyłączenia funkcji procesora, która automatycznie zwiększa wydajność obliczeń prowadzonych równolegle [funkcja zaimplementowana na stałe w BIOS ale aktywna przy procesorze w pełni wspierającym], • Możliwość przypisania w BIOS numeru nadawanego przez Administratora/Użytkownika oraz możliwość weryfikacji tego numeru w oprogramowaniu diagnostyczno-zarządzającym. • Możliwość włączenia/wyłączenia stanu opcji zasilania po uprzedniej utracie, przywrócenie systemu do ostatniego stanu zasilania: • Możliwość zdefiniowania automatycznego uruchamiania komputera w min. dwóch trybach : codziennie lub w wybrane dni tygodnia, • Możliwość ręcznego zdefiniowania stanu uśpienia: <ul style="list-style-type: none"> - tryb uśpienia wyłączony - włączony tylko w S5 - włączony S4 i S5 • Możliwość ręcznego włączenia trybu obrotu wentylatora na pełnych obrotach, automatycznie zostaje wyłączony sterownik wentylatora który pobiera dane środowiskowe za pomocą czujników termicznych, • Możliwość włączenia/wyłączenia wzbudzania komputera za pośrednictwem portów USB, • Możliwość włączania/wyłączania funkcji Wake on Lane • Możliwość ustawienia funkcji Wake on Lane dla WiFi i LAN • Możliwość włączenia/wyłączenia funkcji która umożliwia podczas uśpienia na przesył danych po sieci LAN np. synchronizację e-mail, • Możliwość włączenia/wyłączenia trybu Fastboot, • Możliwość ustawienia trybu Fastboot w opcji : <ul style="list-style-type: none"> - minimalnej – następuje skrócony czas rozruchu komputera z pominięciem pełnej weryfikacji inicjalizacji konfiguracji sprzętowej
--	--

	<p>- gruntownej - podczas rozruchu komputera następuje pełna weryfikacja i inicjalizacja konfiguracji sprzętowej,</p> <ul style="list-style-type: none"> • Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych włączenia lub wyłączenia Virtual Machine Monitor (VMM) • Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych włączenia lub wyłączenia funkcji VT dla Direct I/O • Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych włączenia lub wyłączenia dodatkowych funkcji sprzętowych Virtual Machine Monitor (MVMM) • Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. • Możliwość włączenia/wyłączenia funkcji umożliwiającej dokonywanie downgrade BIOS, • Możliwość włączenia/wyłączenia funkcji tworzenia recovery BIOS na dysku twardym, • Możliwość włączenia/wyłączenia funkcji zdalnego czyszczenia zawartości dysku twardego przy ponownym bootowaniu, • Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych wpisania na stałe ustawień dla : adresu IP serwera, portu serwera, adres IP klienta sieci, adresu klienta Subnet Mask, adresu klienta Gateway oraz sposobu otrzymywania adresu IP : albo DHCP albo statyczne IP • Funkcja zbierania i zapisywania logów, Możliwość przeglądania i kasowania zdarzeń przebiegu procedury POST. Funkcja ta obejmuje datę i godzinę zdarzeń oraz kody wizualnego systemu diagnostycznego LED. • Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot'owania które umożliwia min. : <ul style="list-style-type: none"> - uruchamianie z system zainstalowanego na HDD - uruchamianie systemy z urządzeń zewnętrznych typu HDD-USB, USB Pendrive, CDRW-USB - uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej - uruchamianie systemu z karty SD (funkcja aktywna automatycznie po zainstalowaniu karty SD w czytniku [w przypadku zainstalowania czytnika kart w komputerze] - uruchomienie graficznego systemu diagnostycznego - wejścia do BIOS
--	--

	<ul style="list-style-type: none"> - upgrade BIOS bez konieczności uruchamiania systemu operacyjnego - zmiany sposobu boot'owania z Legacy na UEFI lub z UEFI na Legacy bez konieczności wchodzenia do BIOS. • Możliwość wyłączania portów USB w tym: <ul style="list-style-type: none"> - wszystkich portów USB 2.0 i 3.0, - tylko portów USB znajdujących się na przednim panelu obudowy, - tylko portów USB znajdujących się na tylnym panelu obudowy. - tylko tylnych portów USB 2.0, porty USB 3.0 na panelu tylnym aktywne, - wszystkich portów USB
Certyfikaty i standardy	<ul style="list-style-type: none"> • Certyfikat ISO9001 dla producenta sprzętu • Deklaracja zgodności CE • Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych • Komputer musi spełniać wymogi normy Energy Star 6.0. <p>Wymagany wpis dotyczący oferowanego komputera w internetowym katalogu http://www.eu-energystar.org lub http://www.energystar.gov</p>
Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 26 dB
Warunki gwarancji	<p>Min. 3-letnia gwarancja producenta świadczona na miejscu u klienta. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego.</p> <p>Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzację producenta komputera. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.</p>
Wsparcie techniczne producenta	<p>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p> <p>Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera.</p>
System operacyjny	<p>Zainstalowany system okienkowy system operacyjny w wersji pozwalającej na podłączenie do domeny, umożliwiający instalację w trybie natywnych aplikacji dedykowanych dla systemu Windows 10. Klucz licencyjny musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego na podstawie dołączonego nośnika bezpośrednio z wbudowanego napędu lub zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego. Oferowany dostarczony system jak i również przy reinstalacji nie może wymagać aktywacji klucza licencyjnego za pośrednictwem telefonu i Internetu).</p>

Złącza i porty	<p>Wbudowane porty:</p> <ul style="list-style-type: none"> • min. 1 x HDMI out • min. 1 x DP out • min. 6 portów USB wyprowadzonych na zewnątrz komputera w tym min 4 porty USB 3.0; min. 2 porty USB 3.0 usytuowane na boku obudowy i 4 portów na tylnym panelu w tym min 2 porty USB 3.0, wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.) • Na przednim panelu min 1 port audio tzw. combo (słuchawka/mikrofon) na tylnym panelu min. 1 port Line-out • karta WiFi • Bluetooth • Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika), • Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki dedykowana dla danego urządzenia; wyposażona w : <ul style="list-style-type: none"> • min. 2 złącza DIMM z obsługą do 16GB DDR3 pamięci RAM, • min. 2 złącza SATA w tym 1 szt SATA 3.0; • min. 1 złącza M.2 • Klawiatura USB w układzie polski programisty • Czytnik kart multimedialnych czytający min. karty SD i MMC • Mysz laserowa USB z sześcioma klawiszami oraz rolką (scroll) min 1000dpi • Nagrywarka DVD +/-RW o prędkości min. 8x • Dołączony nośnik ze sterownikami • Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu.
Dodatkowe oprogramowanie	<p>Dołączone do oferowanego komputera oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające:</p> <ul style="list-style-type: none"> - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, - możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji: <ol style="list-style-type: none"> a. o poprawkach i usprawnieniach dotyczących aktualizacji b. dacie wydania ostatniej aktualizacji c. priorytecie aktualizacji d. zgodność z systemami operacyjnymi

	<p>e. jakiego komponentu sprzętu dotyczy aktualizacja</p> <p>f. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e.</p> <ul style="list-style-type: none"> - wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne - możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga. - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację, kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr) - sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania) - dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml - raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach, zainstalowanych aktualizacjach z dokładnym rozbiorem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.
Oprogramowanie biurowe	<p>Zintegrowany pakiet aplikacji biurowych, w którego skład ma wchodzić min.:</p> <ul style="list-style-type: none"> - edytor tekstów; - arkusz kalkulacyjny; - narzędzie do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami); - narzędzie do przygotowania i prowadzenia prezentacji <p>Wymagania podstawowe:</p> <ul style="list-style-type: none"> - pełna polska wersja językowa interfejsu użytkownika, w tym także systemu interaktywnej pomocy w języku polskim. - powinien mieć system aktualizacji darmowych poprawek bezpieczeństwa, przy czym komunikacja z użytkownikiem powinna odbywać się w języku polskim. - dostępność w Internecie na stronach producenta biuletynów technicznych, w tym opisów poprawek bezpieczeństwa, w języku polskim, a także telefonicznej pomocy technicznej producenta pakietu biurowego świadczonej w języku polskim - publicznie znany cykl życia przedstawiony przez producenta dotyczący rozwoju i wsparcia technicznego – w szczególności w zakresie bezpieczeństwa co najmniej 3 lat od daty zakupu.

- możliwość dostosowania pakietu aplikacji biurowych do pracy dla osób niepełnosprawnych np. słabo widzących, zgodnie z wymogami Krajowych Ram Interoperacyjności (WCAG 2.0);

Edytor tekstów musi umożliwiać:

- Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
- Wstawianie oraz formatowanie tabel.
- Wstawianie oraz formatowanie obiektów graficznych.
- Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).
- Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.
- Automatyczne tworzenie spisów treści.
- Formatowanie nagłówków i stopek stron.
- Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.
- Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
- Określenie układu strony (pionowa/pozioma).
- Wydruk dokumentów.
- Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.
- Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

Arkusz kalkulacyjny musi umożliwiać:

- Tworzenie raportów tabelarycznych –
- Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych –
- Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
- Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)
- Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych.
- Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych –
- Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych
- Wyszukiwanie i zamianę danych

- Wykonywanie analiz danych przy użyciu formatowania warunkowego
- Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
- Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
- Formatowanie czasu, daty i wartości finansowych z polskim formatem
- Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
- Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:

- Przygotowywanie prezentacji multimedialnych, które mogą być prezentowane przy użyciu projektora multimedialnego
- Drukowanie w formacie umożliwiającym robienie notatek –
- Zapisanie jako prezentacja tylko do odczytu.
- Nagrywanie narracji i dołączanie jej do prezentacji
- Opatrywanie slajdów notatkami dla prezentera
- Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
- Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
- Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
- Możliwość tworzenia animacji obiektów i całych slajdów
- Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera

Narzędzie do zarządzania informacją prywatną (poczta elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:

- Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,
- Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych, -
- Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,
- Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,
- Automatyczne grupowanie poczty o tym samym tytule,
- Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,
- Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów,
- Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie,
- Zarządzanie kalendarzem,

	<ul style="list-style-type: none"> - Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników, - Przeglądanie kalendarza innych użytkowników, - Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach, - Zarządzanie listą zadań, - Zlecanie zadań innym użytkownikom, - Zarządzanie listą kontaktów, - Udostępnianie listy kontaktów innym użytkownikom, - Przeglądanie listy kontaktów innych użytkowników, - Możliwość przysyłania kontaktów innym użytkownikom.
--	--

Wykonawca dostarczy komputer do pracy jako kolektor danych badania wysiłkowego o następujących parametrach minimalnych:

Parametr	Konfiguracja minimalna
Zestaw archiwizujący badania	<p>Zawiera:</p> <ul style="list-style-type: none"> • Minimalne parametry: Komputer, 16 GB pamięci RAM, dysk twardy 512 GB w RAID, karta sieciowa 100/1000 Mbps, system operacyjny, monitor lub dostęp terminalowy; • Oprogramowanie rejestrowania i ponownego odtwarzania zapisanego badania; • Interfejs do bieżni elektrycznej; • Oprogramowanie do archiwizacji.

System do badań wysiłkowych

Skład systemu	
1.	Zestaw komputerowy z oprogramowaniem do przeprowadzania prób wysiłkowych – 1 kpl. Jak wyżej.
2.	Bezprzewodowy moduł EKG – 1 szt.
Funkcjonalność systemu	
1.	Możliwość wykonywania badań spoczynkowych lub wysiłkowych
2.	Stałe monitorowanie 12 standardowych odprowadzeń uzupełnionych obliczanymi odprowadzeniami ortogonalnymi X, Y, Z
3.	Monitorowanie 15 odprowadzeń z możliwością wyboru: 1 powiększony, 3, 6, 2x6, 3x4, wszystkie kanały EKG na ekranie
4.	Automatyczny pomiar MET, ilości pobudzeń komorowych, HR, poziomu ST, nachylenia odcinka ST oraz różnicy pomiędzy bieżącym a spoczynkowym poziomem ST we wszystkich odprowadzeniach
5.	Automatyczne rozpoznawanie arytmii
6.	Bieżąca analiza zmiany zapisu EKG w stosunku do zapisu wyjściowego dla wszystkich 15 odprowadzeń wraz z możliwością obserwacji powiększonych zespołów średnich
7.	Wiarygodna bieżąca obserwacja i ocena odcinka ST
8.	Możliwość ustawienia punktu J automatycznie i manualnie
9.	Obsługa standardowych protokołów badań: Bruce, Bruce zmodyfikowany itp., protokołu typu RAMP oraz własnych



10.	Możliwość konfiguracji raportów końcowych
11.	Możliwość tworzenia raportów indywidualnych
12.	Ciągłe monitorowanie oraz porównywanie docelowej i aktualnej częstości akcji serca
13.	Wyświetlanie całkowitego czasu badania oraz czasów poszczególnych etapów
14.	Ciągłe monitorowanie prędkości oraz nachylenia bieżni
15.	Prezentacja na bieżąco współczynnika MET i produktu podwójnego
16.	Prezentowanie aktualnego oraz procentowego limitu tętna w stosunku do wartości maksymalnej
17.	Możliwość wprowadzania wyników pomiaru ciśnienia krwi w czasie trwania badania
18.	Możliwość wyboru filtrów górno- i dolnoprzepustowych
19.	Możliwość sterowania przebiegiem badania: wydrukiem raportów, sterowania bieżnią, podglądem w czasie trwania badania
20.	Możliwość zmiany obciążenia podczas badania – prędkość bieżni oraz nachylenie
21.	Możliwość konfiguracji formatu raportu końcowego zawierającego: nazwę stosowanego protokołu, dane pacjenta, czas trwania próby, wartość ciśnienia tętniczego, wartość częstości rytmu serca, maksymalne zmiany odcinka ST w poszczególnych odprowadzeniach, graficzna i tabelaryczna ocena trendów zmian odcinka ST wraz ze współczynnikami MET, możliwość wydruku wybranych odcinków czasowych ze wszystkich 12 odprowadzeń w czasie trwania badania wysiłkowego, z końca etapów oraz z zaznaczonych zdarzeń kardiologicznych („na życzenie”)
22.	Możliwość przeglądu wykonanej części badania w trakcie jego trwania z jednoczesnym podglądem jednego z wybranych odprowadzeń
23.	Możliwość prowadzenia długotrwałego monitorowania spoczynkowego EKG z równoczesną prezentacją częstości akcji serca, zespołów średnich i parametrów odcinka ST
24.	Możliwość przejęcia sterowania obciążeniem przez osobę nadzorującą próbę wysiłkową
25.	Możliwość wpisywania uwag i komentarza końcowego przed zakończeniem badania
26.	Archiwizacja wszystkich danych
27.	Alarmowanie dźwiękiem lub zmianą kolorów odpowiedniego pola dla: przekroczenia zadanego limitu HR, progu poziomu ST oraz nieprawidłowej pracy zadajników obciążenia lub złego kontaktu elektrod
28.	Czułość dla zespołów średnich min. 5, 10, 20, 40 i 100 mm/mV
29.	Prędkość przesuwu zapisu EKG min. 5, 10, 25, 50 i 100 mm/s
30.	Dodawanie zdarzeń EKG podczas przeglądania badania z archiwum
31.	Export bieżącego odcinka EKG widocznego na ekranie monitora do pliku PDF
32.	Tworzenia przez użytkownika szablonów komentarzy dodawanych do badania
33.	Tworzenie profili użytkowników i haseł dostępu
34.	Archiwizacja wyników badań na dysku komputera oraz nośnikach DVD-R/RW
35.	Możliwość współpracy systemu z bieżnią i/lub ergometrem rowerowym
36.	Bezprzewodowe połączenie modułu EKG
37.	Możliwość wymiany poszczególnych przewodów w module EKG
38.	Zasięg transmisji sygnału EKG powyżej 10 m
39.	Tłumienie sygnału wspólnego powyżej 100 dB
40.	Pasmo przenoszenia 0,05 – 150 Hz
41.	Czas pracy modułu EKG z akumulatora min. 16 h
42.	Masa modułu EKG max 400 g
44.	Program i instrukcja obsługi w języku polskim
45.	Obsługa HL7 – współpraca z systemem informatycznym Zamawiającego

2. Komputery przenośne – 2 szt.

Lp.	Nazwa komponentu	Minimalne parametry techniczno-eksploatacyjne (wymagane przez Zamawiającego)
1.	Zastosowanie	Komputer przenośny będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna
2.	Przekątna Ekrenu	Komputer przenośny typu notebook z ekranem min 14" o rozdzielczości: HD (1366 x 768) z podświetleniem LED i powłoką przeciwoodblaskową, jasność 200 nits, kontrast 400:1, maksymalny rozmiar plamki 0,253 mm
3.	Procesor	Procesor powinien osiągać w teście wydajności PassMark Performance Test co najmniej wynik 3927 punktów Passmark CPU Mark. Wynik dostępny na stronie : http://www.passmark.com/products/pt.htm
4.	Płyta główna	Wyposażona przez producenta w dedykowany chipset dla oferowanego procesora. Zaprojektowana na zlecenie producenta i oznaczona trwale na etapie produkcji nazwą lub logiem producenta oferowanego komputera.
5.	Pamięć RAM	4GB (1x4096MB) DDR3L SDRAM 1600MHz możliwość rozbudowy do min 16GB, wymagane min. 2 sloty na pamięci w tym min. jeden wolny
6.	Pamięć masowa	Min. 500GB 7200rpm
7.	Karta graficzna	Zintegrowana w procesorze z możliwością dynamicznego przydzielenia pamięci systemowej, Oferowana karta graficzna musi osiągać w teście PassMark Performance Test co najmniej wynik 799 punktów w G3D Rating, wynik dostępny na stronie : http://www.videocardbenchmark.net/gpu_list.php
8.	Klawiatura	Klawiatura wyspowa z powłoką antybakteryjną, z wbudowanym w klawiaturze podświetleniem z możliwością manualnej regulacji zarówno w BIOS jak i z pod systemu operacyjnego, (układ US -QWERTY), min 100 klawiszy.
9.	Multimedia	dwukanałowa (24-bitowa) karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane głośniki stereo o średniej mocy 2x 2W i szczytowej 2x 2,5W, wbudowany wewnętrzny wzmacniacz głośników.
10.	Bateria i zasilanie	Min. 6-cell [65Whr]. Umożliwiająca jej szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin. Zasilacz o mocy min. 65W
11.	Waga i wymiary	Szerokość: max 380 mm Wysokość: max 25 mm Głębokość: max 260 mm
12.	Obudowa	Szkielet obudowy i zawiasy notebooka wykonany z wzmocnianego metalu. Kąt otwarcia notebooka min 180 stopni.
13.	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji).
14.	BIOS	BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, wymagana pełna obsługa za pomocą klawiatury i myszy lub urządzenia

	<p>wskazującego zintegrowanego (wmontowanego na stałe) w oferowanym urządzeniu</p> <p>Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:</p> <ul style="list-style-type: none"> § wersji BIOS, § nr seryjnego komputera, § numeru wpisanego i nadanego przez administratora (o ile został wpisany, jeśli brak – wymaga się wolnego pola) § dacie produkcji komputera § dacie wysyłki komputera z fabryki § serwisowym kodzie dla komputera nadawanym na etapie produkcji w fabryce § całkowitej wielkości zainstalowanej pamięci RAM, § dostępnej dla systemu pamięci RAM, § prędkości zainstalowanej pamięci RAM § technologii wykonania pamięci RAM § sposobu obsadzenia slotów DIMM z rozbiem na bank A i B (w przypadku obsadzenia tylko jednej kości pamięci drugi bank wolne pole) § typie zainstalowanego procesora § liczbie rdzeni procesora § numerze ID producenta procesora (w celu weryfikacji partii zainstalowanych procesorów) § minimalnej prędkości zegara procesora § maksymalnej prędkości zegara procesora § wielkości pamięci podręcznej procesora L2 cache § wielkości pamięci podręcznej procesora L3 cache § czy jest aktywna w zainstalowanym procesorze technologia wielowątkowości § technologii xx-bit procesora § zainstalowanym i podpiętym HDD (mini SSD) § kontrolerze video § wersji BIOS kontrolera video § pamięci kontrolera video przydzielonej na poziomie BIOS'u § typie zainstalowanego w komputerze panelu LCD (wielkość matrycy w calach) § natywnej rozdzielczości zainstalowanego w komputerze panelu LCD § kontrolerze audio § zainstalowanej karcie Wifi (jeśli brak w wymaganiach specyfikacji dopuszcza się puste pole) § zainstalowanym Bluetooth (jeśli brak w wymaganiach specyfikacji dopuszcza się puste pole) § MAC adresie wbudowanej w płytę główną karty sieciowej § poziomie naładowania baterii zainstalowanej i obecnie użytkowanej w komputerze, § czy komputer pracuje na zasilaniu z baterii lub na podłączonym zasilaczu
--	---

Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznymi urządzeniami.

Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z USB

Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na poziomie systemu, administratora oraz dysku twardego oraz możliwość ustawienia następujących zależności pomiędzy nimi.

Musi posiadać możliwość ustawienia zależności pomiędzy hasłem administratora a hasłem systemowym tak, aby nie było możliwe wprowadzenie zmian w BIOS wyłącznie po podaniu hasła systemowego. Dopuszcza się aby po wprowadzeniu hasła systemowego była możliwość jedynie zmiany hasła systemowego i hasła dla dysku twardego (o ile zostało zdefiniowane przez administratora)

Możliwość włączenia/wyłączenia wbudowanej karty sieciowej LAN

Możliwość włączenia/wyłączenia PXE

Możliwość włączenia/wyłączenia w dowolnej kombinacji (w tym też pojedynczej) zainstalowanych dysków twardego,

Możliwość ręcznego ustawienia trybu pracy zintegrowanego kontrolera SATA w min. trybach :

- wyłączony
- AHCI

Możliwość włączenia/wyłączenia technologii raportowania i zgłaszania błędów zainstalowanego dysku twardego podczas uruchamiania systemu, technologia ta jest analizą samokontrolną,

Możliwość włączenia/wyłączenia zintegrowanego kontrolera USB,

Możliwość włączenia/wyłączenia zintegrowanego kontrolera audio,

Możliwość włączenia/wyłączenia podświetlenia wbudowanego w klawiaturę [funkcja zaimplementowana na stałe w BIOS ale aktywna przy zainstalowanej klawiaturze z wbudowanym podświetleniem],

Możliwość włączenia/wyłączenia urządzeń :

- kamery [funkcja zaimplementowana na stałe w BIOS ale aktywna przy zainstalowanej kamerze],
- czytnika multimedialnych kart,
- mikrofon (funkcja zaimplementowana na stałe w BIOS ale aktywna przy zainstalowanym mikrofonie)

Możliwość ustawienia czytnika kart multimedialnych w opcji tylko odczyt,

Możliwość włączenia/wyłączenia szybkiego ładowania baterii

Możliwość włączenia/wyłączenia funkcjonalności Wake On LAN/WLAN – zdalne uruchomienie komputera za pośrednictwem sieci LAN i WLAN – min. trzy opcje do wyboru: tylko LAN, tylko WLAN, LAN oraz WLAN,

Możliwość włączenia/wyłączenia hasła dla dysku twardego,

Możliwość ustawienia jasności matrycy podczas pracy, oddzielnie dla baterii i dla zasilacza,

Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych włączenia lub wyłączenia Virtual Machine Monitor (VMM)

[funkcja zaimplementowana na stałe w BIOS ale aktywna przy procesorze w pełni wspierającym VMM]

Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych włączenia lub wyłączenia funkcji VT dla Direct I/O [funkcja zaimplementowana na stałe w BIOS ale aktywna przy procesorze w pełni wspierającym funkcję VT dla Direct I/O]

Możliwość ręcznego zdefiniowania zapotrzebowania na ilość rdzeni procesora dla aplikacji a w szczególności dla starszych, mających problemy z nowymi procesorami, wymagane min. dwa tryby :

- aktywny jeden rdzeń
- aktywne dwa rdzenie

Możliwość ręcznego włączenia/wyłączenia funkcji, która pozwalająca na dynamiczną zmianę wartości [mnożnika](#) i [napięcia](#) [funkcja związana z architekturą procesora, nie dopuszcza się overclockingu, zaimplementowana na stałe w BIOS ale aktywna przy procesorze w pełni wspierającym],

Możliwość ręcznego włączenia/wyłączenia funkcji uśpienia procesora dla systemu operacyjnego w trybie bezczynności w celu zwiększenia oszczędności energii [funkcja zaimplementowana na stałe w BIOS ale aktywna przy procesorze w pełni wspierającym]

Możliwość ręcznego włączenia/wyłączenia funkcji procesora, która automatycznie zwiększa [taktowanie procesora](#), gdy [komputerowi](#) potrzebna jest wyższa prędkość obliczeniowa [funkcja zaimplementowana na stałe w BIOS ale aktywna przy procesorze w pełni wspierającym],

Możliwość ręcznego włączenia/wyłączenia funkcji procesora, która automatycznie zwiększa wydajność obliczeń prowadzonych równolegle [funkcja zaimplementowana na stałe w BIOS ale aktywna przy procesorze w pełni wspierającym],

Możliwość przypisania w BIOS numeru nadawanego przez Administratora/Użytkownika oraz możliwość weryfikacji tego numeru w oprogramowaniu diagnostyczno-zarządzającym.

- Możliwość włączenia/wyłączenia układu TPM.
- Możliwość ustawienia trybu Fastboot w opcji :
 - minimalnej – następuje skrócony czas rozruchu komputera z pominięciem pełnej weryfikacji inicjalizacji konfiguracji sprzętowej
 - gruntownej - podczas rozruchu komputera następuje pełna weryfikacja i inicjalizacja konfiguracji sprzętowej

Funkcja zbierania i zapisywania logów, Możliwość przeglądania i kasowania zdarzeń przebiegu procedury POST. Funkcja ta obejmuje datę i godzinę zdarzeń

Możliwość włączenia/wyłączenia zabezpieczenie wykrywające uszkodzenie zasilacza lub wykrycie podłączenia zasilacza o niewłaściwym min. napięciu,

Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne.

		<p>Możliwość zdefiniowania automatycznego uruchamiania komputera w min. dwóch trybach : codziennie lub w wybrane dni tygodnia</p> <p>Możliwość włączenia/wyłączenia wzbudzania komputera za pośrednictwem portów USB</p> <p>Możliwość włączenia/wyłączenia funkcji umożliwiającej dokonywanie downgrade BIOS,</p> <p>Możliwość włączenia/wyłączenia funkcji tworzenia recovery BIOS na dysku twardym,</p> <p>Możliwość włączenia/wyłączenia funkcji zdalnego czyszczenia zawartości dysku twardego przy ponownym bootowaniu,</p> <p>Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot'owania które umożliwia min. :</p> <ul style="list-style-type: none"> - uruchamianie z system zainstalowanego na HDD - uruchamianie systemu z urządzeń zewnętrznych typu HDD-USB, USB Pendrive, CDRW-USB - uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej - uruchamianie systemu z karty SD (funkcja aktywna automatycznie po zainstalowaniu karty SD w czytniku) - uruchomienie graficznego systemu diagnostycznego - wejścia do BIOS - upgrade BIOS bez konieczności uruchamiania systemu operacyjnego - zmiany sposobu boot'owania z Legacy na UEFI lub z UEFI na Legacy bez konieczności wchodzenia do BIOS.
15.	Certyfikaty	<p>Certyfikat ISO9001:2000 dla producenta sprzętu (należy załączyć do oferty)</p> <p>Certyfikat ISO 14001 dla producenta sprzętu (należy załączyć do oferty)</p> <p>Deklaracja zgodności CE (załączyć do oferty)</p> <p>Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki</p> <p>Potwierdzenie kompatybilności komputera na stronie Windows Logo'd Products List na daną platformę systemową (wydruk ze strony)</p> <p>EnergyStar 6.1 – załączyć do oferty certyfikat lub oświadczenie wykonawcy opatrzone numerem postępowania oraz poparte oświadczeniem producenta.</p>
16.	Ergonomia	<p>Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 17dB (załączyć do oferty oświadczenie wykonawcy opatrzone numerem postępowania oraz poparte oświadczeniem producenta)</p> <p>Oferowany komputer musi spełniać poniższe wymaganie odnośnie zakresu temperatur :</p> <ul style="list-style-type: none"> - praca – od 0 do 35 °C - magazynowanie - od -40 do 65 °C <p>[załączyć do oferty oświadczenie wykonawcy opatrzone numerem postępowania oraz poparte oświadczeniem producenta]</p>

17.	Diagnostyka	<p>Wbudowany system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot umożliwiający jednocześnie przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanej komputerze bez konieczności uruchamiania systemu operacyjnego. System opatrzony min. o funkcjonalność :</p> <ul style="list-style-type: none"> - wykaz wszystkich zainstalowanych komponentów z numerami seryjnymi dla : - płyty głównej, - pamięci - HDD - kamery - modemu 3G/LTE - dokładnych informacji o zainstalowanej baterii, a w szczególności : <ul style="list-style-type: none"> - ilości wykonanych cykli ładowania baterii - temperaturze baterii - podanej w % wartości żywotności baterii - Test podzespołów : <ul style="list-style-type: none"> - test podpiętych kabli, - test magistrali PCIe - test matrycy LCD, - test głośnika - test dysku twardego - test partycji rozruchowej systemu OS - test portów USB - test kamery - test karty graficznej - test baterii - test zasilacza - test wentylatora procesora - test procesora - test pamięci <p>Wbudowany wizualny system diagnostyczny oparty na sygnalizacji za pomocą diod sygnalizujących pracę HDD, zasilania, WiFi umożliwiający wykrycie bez konieczności uruchamiania systemu operacyjnego min.:</p> <ul style="list-style-type: none"> - awarii procesora, - błędu pamięci, - problemu z inicjalizacją systemu OS z HDD, - awarii karty graficznej, - awarii portów USB, - braku pamięci, - problemu z panelem LCD - problemu z zainicjowaniem/obsługą pamięci
18.	Bezpieczeństwo	<p>Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu powoduje uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych</p>

		<p>dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego.</p> <p>Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej.</p> <p>Czujnik spadania zintegrowany z płytą główną działający nawet przy wyłączonym notebooku oraz konstrukcja absorbująca wstrząsy</p> <p>Czytnik linii papilarnych</p> <p>Złącze typu Kensington Lock</p>
19.	System operacyjny	<p>Zainstalowany system operacyjny Windows 10 Professional lub + nośnik, klucz licencyjny Windows 10 Professional musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego na podstawie dołączonego nośnika bezpośrednio z wbudowanego napędu lub zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego. Oferowany dostarczony system jak i również przy reinstalacji nie może wymagać aktywacji klucza licencyjnego za pośrednictwem telefonu i Internetu)</p>
20.	Porty i złącza	<p>Wbudowane porty i złącza :</p> <ul style="list-style-type: none"> - 1x VGA - 1x HDMI 1.4 - 1x RJ-45 (10/100/1000) - 2x USB 3.0 - 1x USB 2.0 - czytnik kart multimedialny wspierający karty SD 4.0 - czytnik linii papilarnych - współdzielone złącze słuchawkowe stereo i złącze mikrofonowe tzw. combo - port zasilania - touchpad z strefą przewijania w pionie, poziomie wraz z obsługą gestów - Zintegrowana w postaci wewnętrznego modułu karta sieci WLAN - moduł bluetooth 4.0 dopuszcza się współdzielony z kartą WiFi
21.	Warunki gwarancyjne	<p>3-letnia gwarancja producenta świadczona na miejscu u klienta, Czas reakcji serwisu - do końca następnego dnia roboczego.</p> <p>Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta</p>

3. Urządzenia drukujące i skanery – urządzenia wielofunkcyjne – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Funkcje	Drukowanie / kopiowanie / skanowanie
Pamięć standardowa	128 MB
Interfejsy	Hi-Speed USB 2.0, Ethernet 10 / 100 Base-TX
Maks. miesięczny cykl obciążenia	12 000 stron
Szybkość druk czarno-biały	Min. 28 str/min A4 mono
Rozdzielczość drukowania	Min. Do 4 800 x 600 dpi rozdzielczości efektywnej
Drukowanie dwustronne	Tak

Emulacja	PCL6 / PCL5e
Kopiowanie - powiększenie	25–400% (podajnik automatyczny, szyba)
Kopiowanie wielokrotne	1-99 stron
Funkcje kopiowania	Kopiowanie dokumentów tożsamości, 2 kopie na jednej stronie, 4 kopie na jednej stronie, kopiowanie plakatów, automatyczne dopasowanie
Skanowanie - metoda	Kolor CIS
Skanowanie kompatybilność	Standard Twain / standard WIA
Skanowanie rozdzielczość	Min. Optyczna rozdzielczość 1 200 x 1 200 dpi
Funkcje skanowania	Klient (PC)
Kaseta	Standardowa kaseta na 250 arkuszy Podajnik uniwersalny na 1 arkusz
Pojemność odbiornika	Min. 120 arkuszy drukiem do dotu
ADF	Tak, na min. 40 arkuszy
Panel operacyjny	2-wierszowy LCD
Poziom hałasu	Drukowanie poniżej 50 dBA / kopiowanie poniżej 54 dBA / Tryb gotowości poniżej 26 dBA
Gwarancja	3-letnia gwarancja producenta

4. Urządzenia drukujące kolor – 1 szt.

<i>Nazwa komponentu</i>	<i>Wymagane minimalne parametry techniczne</i>
Obszar zastosowania	Atramentowa, bez wystających elementów, zwarta konstrukcja
Druk w kolorze	TAK
Prędkość druku w czerni (maksymalna)	Min. 22 str/min
Maksymalna wydajność	Min. 450 str./miesiąc
Jakość druku w czerni	Min. 1200x600 dpi
Wkłady zamienne (czarny)	Min. na 500 str.
Podajnik	Min. 50 arkuszy A4
Funkcje łączności	- USB - bezprzewodowa karta sieciowa - możliwość drukowania bezpośrednio z urządzeń przenośnych
Obsługa papieru	- standardowa pojemności podajnika papieru – min. 40 str. - Obsługiwane formaty – min. A4, A5, koperty (A2, C5, C6) - obsługiwana gramatura papieru – min. od 70 do 200 g/m ²
Zasilanie i środowisko	- Napięcie wejściowe: 200–240 V, 50–60 Hz - zużycie energii max. 20 W (aktywność) - sprawność energetyczna - Certyfikat ENERGY STAR® - zakres temperatur podczas eksploatacji – min. 5–40°C
Gwarancja	Min. 3 lata

5. Urządzenia drukujące mono – 4 szt. (w tym jedna przy biletowacie)

Nazwa komponentu	Wymagane minimalne parametry techniczne
Obszar zastosowania	Przenośna, laserowa, bez wystających elementów, zwarta konstrukcja
Prędkość druku w czerni (maksymalna)	Min. 22 str/min
Maksymalna wydajność	Min. 450 str./miesiąc
Jakość druku w czerni	Min. 1200x600 dpi
Wkłady zamienne (czarny)	Min. na 500 str.
Podajnik	Min. 50 arkuszy A4
Funkcje łączności	- USB - bezprzewodowa karta sieciowa - możliwość drukowania bezpośrednio z urządzeń przenośnych
Obsługa papieru	- standardowa pojemności podajnika papieru – min. 40 str. - Obsługiwane formaty – min. A4, A5, koperty (A2, C5, C6) - obsługiwana gramatura papieru – min. od 70 do 200 g/m ²
Zasilanie i środowisko	- Napięcie wejściowe: 200–240 V, 50–60 Hz - zużycie energii max. 20 W (aktywność) - sprawność energetyczna - Certyfikat ENERGY STAR® - zakres temperatur podczas eksploatacji – min. 5–40°C - możliwość działania na akumulatorze dołączonym do drukarki
Gwarancja	Min. 3 lata

6. Skaner – 2 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Funkcje	Skanowanie
Interfejsy	Hi-Speed USB 2.0, Ethernet 10 / 100 Base-TX
Skanowanie - metoda	Kolor CIS
Skanowanie kompatybilność	Standard Twain / standard WIA
Skanowanie rozdzielczość	Min. Optyczna rozdzielczość 1 200 x 1 200 dpi
Funkcje skanowania	Klient (PC)
ADF	Tak, na min. 40 arkuszy
Gwarancja	3-letnia gwarancja producenta

7. Tablety – 6 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Ekran	- ekran dotykowy: min. 10" - rozdzielczość ekranu: min. 1024x768 - jasność: min 500 nitów
System operacyjny	Min. Android 4.2
Procesor	Dual-Core min. 1,5 GHz
Pamięć RAM	Min. 1 GB
Pamięć	- wewnętrzna min. 16GB

Łączność bezprzewodowa	- 802.11 a/b/g/n - wbudowany modem min. 3G - bluetooth 4.0
Czytnik kodów kreskowych	1D i 2 D
Kamera	- min tył 5Mp, przód 1,2 Mp
Audio	wbudowany głośnik
Bateria	- pojemność baterii umożliwiającą do min. 7 godzin pracy - możliwość wymiany baterii (Hot-swap)
Zasilanie	100-240 VAC
Temperatura pracy	Min. -5 to +45°C
Wytrzymałość	- min. IP 54 - odporność na upadek zapewniony przez obudowę lub nakładkę gumową na obudowę.
Waga	Max. 1,5 kg
Dodatkowe wyposażenie	Stacja dokująca
Gwarancja	3 lata

Ad 3. Rozbudowa systemu EDM (HRF II.3)

a. Elektroniczna Dokumentacja Medyczna (EDM) (SW 5.4.I.3.4);

Ze względu, iż Zamawiający posiada już wdrożoną podstawową funkcjonalność systemu EDM, zakres rozbudowy systemu EDM zostanie ustalony na etapie analizy przedwdrożeniowej. Przedmiotem zamówienia w tym zakresie, jest dokonanie analizy celem dostosowania parametrów i funkcjonalności wdrożonego oprogramowania EDM (projekt Mazowieckie e-zdrowie) do wymogów CSIOZ oraz wykonania Interfejsów zgodnie z Załącznikiem nr 4 do OPZ – Instrukcja stosowania Polskiej implementacji krajowej HL7 CDA w systemach EDM.

Ad 4. Modernizacja środowiska serwerowego (HRF II.4)

a. modernizacja użytkowanego środowiska przetwarzania danych – serwery, macierze, w tym zakup nowego wyposażenia (SW 5.4.I.1.4);

W ramach sprzętu serwerowego muszą zostać wygenerowane platformy, przeznaczone do kolektorów wymiany danych, pomiędzy poszczególnymi urządzeniami o następujących wymaganiach minimalnych:

I. Kolektor danych badania endoskopowego – 1 szt.

Parametr	Konfiguracja minimalna
Zestaw archiwizujący badania	Zawiera:

	<ul style="list-style-type: none"> Minimalne parametry: Komputer lub system wirtualny, minimalne wymagania: procesor czterordzeniowy lub dostępne 4 rdzenie procesora wirtualnego, 16 GB pamięci RAM, dysk twardy 512 GB w RAID, karta sieciowa 100/1000 Mbps, system operacyjny, monitor lub dostęp terminalowy; oprogramowanie specjalistyczne; Umożliwienie zainstalowania interfejsu do wideobronchofiberoskopu; Monitor HD; Oprogramowanie do archiwizacji.
--	--

II. Kolektor danych badania EKG – 1 szt.

Parametr	Konfiguracja minimalna
Zestaw archiwizujący badania	<p>Zawiera:</p> <ul style="list-style-type: none"> Minimalne parametry: Komputer lub system wirtualny, minimalne wymagania: procesor czterordzeniowy lub dostępne 4 rdzenie procesora wirtualnego, 16 GB pamięci RAM, dysk twardy 512 GB w RAID, karta sieciowa 100/1000 Mbps, system operacyjny, monitor lub dostęp terminalowy; Oprogramowania specjalistyczne; Możliwość podłączenia interfejsu do 3 rejestratorów analizy EKG; Oprogramowanie do archiwizacji.

III. Kolektor danych badania ciśnienia tętniczego- 1 szt.

Parametr	Konfiguracja minimalna
Zestaw archiwizujący badania	<p>Zawiera:</p> <ul style="list-style-type: none"> Minimalne parametry: Komputer lub system wirtualny, minimalne wymagania: procesor czterordzeniowy lub dostępne 4 rdzenie procesora wirtualnego, 16 GB pamięci RAM, dysk twardy 512 GB w RAID, karta sieciowa 100/1000 Mbps, system operacyjny, monitor lub dostęp terminalowy; Oprogramowanie specjalistyczne; Możliwość podłączenia interfejsu do 2 rejestratorów ciśnienia tętniczego; Oprogramowanie do archiwizacji.

IV. Kolektor danych zaburzeń oddychania – 1 szt.

Parametr	Konfiguracja minimalna
Zestaw archiwizujący badania	<p>Zawiera:</p> <ul style="list-style-type: none"> Minimalne parametry: Komputer lub system wirtualny, minimalne wymagania: procesor czterordzeniowy lub dostępne 4 rdzenie procesora wirtualnego, 16 GB pamięci RAM, dysk twardy 512 GB w RAID, karta sieciowa 100/1000

	<p>Mbps, system operacyjny, monitor lub dostęp terminalowy;</p> <ul style="list-style-type: none"> • System cyfrowego rejestratora • oprogramowanie specjalistyczne; • Oprogramowanie do archiwizacji.
--	---

V. Kolektor danych diagnostyki obrazowej – 1 szt.

Parametr	Konfiguracja minimalna
Zestaw archiwizujący badania	<p>Zawiera:</p> <ul style="list-style-type: none"> • Minimalne parametry: Komputer lub system wirtualny, minimalne wymagania: procesor czterordzeniowy lub dostępne 4 rdzenie procesora wirtualnego, 16 GB pamięci RAM, dysk twardy 512 GB w RAID, karta sieciowa 100/1000 Mbps, system operacyjny, monitor lub dostęp terminalowy; • Oprogramowanie specjalistyczne; • Interfejs do sondy do przeprowadzania badania echa serca • Oprogramowanie do archiwizacji.

VI. Kolektor danych diagnostyki obrazowej – 1 szt.

Parametr	Konfiguracja minimalna
Zestaw archiwizujący badania	<p>Zawiera:</p> <ul style="list-style-type: none"> • Minimalne parametry: Komputer lub system wirtualny, minimalne wymagania: procesor czterordzeniowy lub dostępne 4 rdzenie procesora wirtualnego, 16 GB pamięci RAM, dysk twardy 512 GB w RAID, karta sieciowa 100/1000 Mbps, system operacyjny, monitor lub dostęp terminalowy; • Oprogramowanie specjalistyczne; • Interfejs do aparatu laboratoryjnego • Oprogramowanie do archiwizacji.

Komponent	Minimalne wymagania Serwer RACK – 4 szt.
Obudowa	Obudowa typu Rack o wysokości maksymalnie 1U z możliwością instalacji minimum 8 dysków 2.5" Hot Plug wraz z kompletem szyn umożliwiających montaż w szafie rack, wysuwanie serwera do celów serwisowych wraz z organizatorem kabli.
Płyta główna	Z możliwością instalacji minimum dwóch fizycznych procesorów, posiadająca minimum 24 sloty na pamięci z możliwością zainstalowania do minimum 1.5 TB pamięci RAM, możliwe zabezpieczenia pamięci: ECC, SDDC, Memory Mirroring Rank Sparing, SBEC. Płyta główna zaprojektowana przez producenta serwera i oznaczona trwale jego znakiem firmowym.
Procesor	Zainstalowane dwa procesory min. ośmiordzeniowe dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku minimum 632 punktów w teście SPECint_rate_base2006 dostępnym na stronie internetowej www.spec.org dla konfiguracji dwuprocesorowej.
Pamięć RAM	Minimum 256 GB pamięci typu RDIMM o częstotliwości taktowania minimum 2400 MHz RAM
Sloty PCI Express	- min. 2 sloty x16 generacji 3 połowy wysokości i połowy długości, - min. 1 slot x8 generacji 3 połowy wysokości i połowy długości
Wbudowane porty	Minimum 5 portów USB 2.0 z czego min. 2 w technologii 3.0 (porty nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń) 1x RS-232, 2x VGA D-Sub
Karta graficzna	Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1280x1024 pikseli
Interfejsy sieciowe	Minimum dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie SFP+, interfejsy sieciowe nie mogą zajmować żadnego z dostępnych slotów PCI Express oraz złącz USB. Możliwość instalacji wymiennie modułów udostępniających: - dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie BaseT - cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT. - cztery interfejsy sieciowe 10Gb Ethernet w standardzie SFP+
Napęd optyczny	Brak zainstalowanego wewnętrznego napędu optycznego
Kontroler dyskowy	Brak zainstalowanego wewnętrznego kontrolera dyskowego.
Wewnętrzna pamięć masowa	Możliwość instalacji dysków twardych typu: SATA, SSD dostępnych w ofercie producenta serwera. Zainstalowana dodatkowa wewnętrzna pamięć typu flash, o pojemności min. 16GB, dedykowana dla hypervisora wirtualizacyjnego, umożliwiająca konfigurację zabezpieczenia typu "mirror" lub RAID 1, rozwiązanie nie może powodować zmniejszenia minimalnej ilości wewnętrznej pamięci masowej w serwerze.
System operacyjny	Brak systemu operacyjnego.
Bezpieczeństwo i system diagnostyczny	- Elektroniczny panel informacyjny umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze, adresach MAC kart sieciowych, numerze serwisowym serwera, aktualnym zużyciu energii, nazwie serwera, modelu serwera. - Fabryczne oznaczenie urządzenia, wykonane przez producenta serwera informujące Zamawiającego m.in. o numerze serwisowym serwera, pełnej nazwie podmiotu Zamawiającego, modelu serwera; gwarantujące Zamawiającemu dostawę nowego, nieużywanego i nie pochodzącego z innych projektów sprzętu.

	<ul style="list-style-type: none"> - Zintegrowany z płytą główną moduł TPM - Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. - Fizyczne zabezpieczenie dedykowane przez producenta serwera uniemożliwiające wyjęcie dysków twardych umieszczonych na froncie obudowy przez nieuprawnionych użytkowników.
Chłodzenie i zasilanie	<p>Minimum sześć wewnętrznych redundantnych wentylatorów typu Hot Plug</p> <p>Dwa redundantne zasilacze Hot Plug o mocy minimum 750 Wat każdy wraz z kablami o dł. Min. 2m</p>
Zarządzanie	<p>Niezależna od zainstalowanego systemu operacyjnego, zintegrowana z płytą główną posiadająca port RJ45 lub jako dodatkowa karta rozszerzeń (Zamawiający dopuszcza zastosowanie karty instalowanej w slotcie PCI Express jednak nie może ona powodować zmniejszenia minimalnej ilości wymaganych slotów w serwerze), posiadająca minimalną funkcjonalność :</p> <ul style="list-style-type: none"> - komunikacja poprzez dedykowany interfejs RJ45 - podstawowe zarządzanie serwerem poprzez protokół IPMI 2.0, SNMP, VLAN tagging - wbudowana diagnostyka - wbudowane narzędzia do instalacji systemów operacyjnych - dostęp poprzez interfejs graficzny Web karty oraz z linii poleceń - monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji - lokalna oraz zdalna konfiguracja serwera - zdalna instalacja systemów operacyjnych - wsparcie dla IPv4 i IPv6 - zapis zrzutu ekranu z ostatniej awarii - integracja z Active Directory - wirtualna konsola z dostępem do myszy i klawiatury - udostępnianie wirtualnej konsoli - autentykacja poprzez publiczny klucz (dla SSH) - możliwość obsługi poprzez dwóch administratorów równocześnie - wysyłanie do administratora powiadomienia o awarii lub zmianie konfiguracji sprzętowej <p>Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:</p> <ul style="list-style-type: none"> - Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych - Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta - Wsparcie dla protokołów– WMI, SNMP, IPMI, WSMAN, Linux SSH - Możliwość oskryptowywania procesu wykrywania urządzeń - Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram - Szczegółowy opis wykrytych systemów oraz ich komponentów - Możliwość eksportu raportu do CSV, HTML, XLS - Grupowanie urządzeń w oparciu o kryteria użytkownika - Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach - Automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń - Szybki podgląd stanu środowiska - Podsumowanie stanu dla każdego urządzenia - Szczegółowy status urządzenia/elementu/komponentu - Generowanie alertów przy zmianie stanu urządzenia

	<ul style="list-style-type: none"> - Filtry raportów umożliwiające podgląd najważniejszych zdarzeń - Integracja z service desk producenta dostarczonej platformy sprzętowej - Możliwość przejęcia zdalnego pulpitu - Możliwość podmontowania wirtualnego napędu - Automatyczne zaplanowanie akcji dla poszczególnych alertów w tym automatyczne tworzenie zgłoszeń serwisowych w oparciu o standardy przyjęte przez producentów oferowanego w tym postępowaniu sprzętu - Kreator umożliwiający dostosowanie akcji dla wybranych alertów - Możliwość importu plików MIB - Przesyłanie alertów „as-is” do innych konsol konsol firm trzecich - Możliwość definiowania ról administratorów - Możliwość zdalnej aktualizacji sterowników i oprogramowania wewnętrznego serwerów - Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) - Możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta - Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów - Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych
Gwarancja	Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Możliwość rozszerzenia gwarancji przez producenta do siedmiu lat.
Certyfikaty	<p>Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001</p> <p>Serwer musi posiadać deklaracja CE (dokument załączyć do oferty)</p> <p>Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2008 R2, Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2.</p> <p>Zgodność z wirtualizatorami Citrix, Vmware vSphere, Microsoft Hyper-V.</p> <p>Zgodność z systemami SUSE Linux Enterprise Server, RedHat Enterprise Linux, Citrix XenServer, VMware vSphere, Sun Solaris.</p>

Macierz dyskowa – 1 szt.

Komponent	Minimalne wymagania
Macierz	Macierz powinna posiadać dwa redundantne kontrolery macierzowe wraz z 24 dyskami o maksymalnej wysokości 2U, Macierz musi umożliwiać rozbudowę o moduły 12 dysków 3,5” oraz 24 dyski 2,5” Obsługa minimum 192 dysków SAS/NLSAS lub SSD.
Wymagana przestrzeń	Macierz musi być wyposażona w: 6 dysków 2,5” o pojemności 480 GB (SSD 12Gb/s) 18 dysków 2,5” o pojemności 1.8 TB (SAS 12Gb/s, o prędkości obrotowej 10k)

Pamięć podręczna (Cache)	Pamięć podręczna (cache) – 16 GB pojemności użytkowej dla danych oraz informacji kontrolnych na każdy kontroler (sumarycznie 32 GB). Nie dopuszcza rozwiązań rozszerzających pamięć podręczną cache dyskami SSD/Flash.
Interfejsy zewnętrzne	Macierz musi być wyposażona w 4 porty iSCSI 10Gb/s, każdy kontroler macierzy w trybie Active-Active.
Dostępność	Odporność na zanik zasilania jednej fazy lub awarię zasilacza macierzy (redundancja układu zasilania).
	Możliwość łączenia w macierzy różnych poziomów RAID: <ul style="list-style-type: none"> a. możliwość zastosowania RAID10, b. możliwość zastosowania RAID5, c. możliwość zastosowania RAID6
	Podwójne niezależne przyłącza SAS 6Gb/s do wewnętrznych napędów dyskowych.
	Odporność na awarię pamięci cache – lustrzany zapis danych oraz technologia zapewniająca ochronę danych z pamięci cache w razie utraty zasilania.
	Zdublowanie pozostałych komponentów macierzy, takich jak: kontrolery, wewnętrzne szyny/przełączniki, wentylatory.
Wspierane systemy operacyjne	Możliwość wykonywania wszystkich napraw, rekonfiguracji, rozbudowy i upgrade'ów (zarówno sprzętu jak i oprogramowania macierzy) w trybie online (bez przerywania pracy systemu).
	Wymagane wsparcie dla różnych systemów operacyjnych, co najmniej AIX, HP-UX, MS Windows, VMware oraz Linux
	Wsparcie dla mechanizmów dynamicznego przełączania zadań I/O pomiędzy kanałami w przypadku awarii jednego z nich (path failover). Wymagane jest wsparcie dla odpowiednich mechanizmów oferowanych przez producentów systemów operacyjnych: AIX, HP-UX, MS Windows, Vmware, Linux.
	Macierz musi mieć wsparcie dla automatycznego, bez agenta, odzyskiwania bloków (space reclamation) dla systemu operacyjnego Linux i systemu plików EXT4, NTFS dla Windows 2012, VMFSv5 dla ESX oraz VxFS w przypadku zastosowania technologii Thin Provisioning.
Skalowalność	Wykonywanie rozbudowy sprzętowej w trybie online.
	Umożliwia rozbudowę do minimum 192 dysków 2,5".
	Możliwość rozbudowy macierzy za pomocą nowych dysków o większych pojemnościach oraz dysków typu SSD/Flash – zoptymalizowanych pod kątem zapisu bądź odczytu
	Macierz musi umożliwiać mieszanie dysków o różnych prędkościach obrotowych w ramach jednej półki dyskowej.
Zarządzanie	Oprogramowanie do zarządzania macierzą przez administratora klienta – graficzny interfejs do monitorowania stanu i konfiguracji macierzy, diagnostyki, mapowania zasobów do serwerów (zarówno podłączanych bezpośrednio jak i przez sieć SAN – LUN Masking).
	Stałe monitorowanie macierzy przez zdalne centrum serwisowe.
	Monitorowanie wydajności macierzy według parametrów takich jak: przepustowość oraz liczba operacji I/O dla interfejsów zewnętrznych, wolumenów logicznych LUN, oraz kontrolerów.

	Wymagana możliwość zbierania i przechowywania informacji o wydajności macierzy.
	Możliwość konfigurowania wolumenów logicznych LUN o pojemności użytkowej 250TB.
	Macierz musi posiadać wbudowaną funkcjonalność typu thin provisioning umożliwiającą alokację wirtualnej przestrzeni dyskowej, do której fizyczne dyski mogą być dostarczone w przyszłości.
Możliwość migracji danych w obrębie macierzy	Konieczne jest posiadanie możliwości uruchomienia automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane między różnymi typami dysków oraz różnymi poziomami RAID w zależności od stopnia obciążenia macierzy dyskowej. Dane często używane macierz powinny automatycznie przemieszczać na dyski o największej prędkości obrotowej, dane rzadko używane na dyski o prędkości obrotowej najniższej.
	Macierz musi mieć możliwość migracji wolumenów logicznych LUN pomiędzy różnymi grupami dyskowymi RAID w obrębie macierzy. Migracja musi być wykonywana w trybie on-line. Jeżeli funkcjonalność taka wymaga dodatkowej licencji, to należy je uwzględnić w ofercie.
	Macierz musi umożliwiać tworzenie jednego wolumenu logicznego LUN w obrębie wszystkich produkcyjnych dysków macierzy. Jeżeli funkcjonalność taka wymaga dodatkowej licencji, to należy je uwzględnić w ofercie. Musi również umożliwiać udostępnienie tego wolumenu logicznego LUN po protokole FC
Lokalna replikacja danych	Możliwość tworzenia kopii danych z poziomu macierzy i wewnątrz macierzy bez angażowania systemu operacyjnego hosta.
	Możliwość tworzenia i utrzymywania jednocześnie minimum ośmiu lokalnych kopii danych wewnątrz macierzy dla każdego urządzenia LUN (tzw. kopie point-in-time) przez administratora.
	Oferowana macierz dyskowa musi umożliwiać wykonanie lokalnej kopii danych na całej zaoferowanej przestrzeni dyskowej.
	Wymaga jest również funkcjonalność wykonywania kopii wirtualnych typu snapshot. Jest wymagana licencja na pełną pojemność macierzy oraz maksymalną ilość snapshotów w obrębie macierzy.
	Kopie migawkowe muszą mieć możliwość prezentacji, jako urządzenia LUN w trybie do odczytu i zapisu. Jeżeli ta funkcjonalność wymaga dodatkowej licencji należy ją dostarczyć.
Współpraca z aplikacjami	Możliwość integracji środowiska VMware, Microsoft SQL z mechanizmem lokalnej replikacji danych.
Zdalna replikacja danych	Macierz musi posiadać funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie synchronicznym oraz asynchronicznym bez użycia dodatkowych serwerów lub innych urządzeń.
	Oprogramowanie musi zapewniać funkcjonalność zawieszania i ponownej przyrostowej resynchronizacji kopii z oryginałem.
	Wymagane do replikacji jest użycie protokołu iSCSI.
	Oferowana macierz dyskowa musi umożliwiać wykonanie w trybie synchronicznym i asynchronicznym zdalnej kopii danych całej powierzchni użytkowej macierzy.

Importowanie danych	Macierz musi posiadać funkcjonalność onlinowego importu danych z macierzy innego producenta z jednoczesną konwersją wolumenu logicznego LUN do trybu „Thin Provision”
Gwarancja	Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czterogodzinnym czasem reakcji od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Możliwość rozszerzenia gwarancji przez producenta do siedmiu lat.
Wymiana dysków	Wymiana dysków może być dokonywana przez klienta.
Instalacja	Cena macierzy musi zawierać usługę implementacji dla min. 8 hostów przeprowadzoną przez producenta lub autoryzowany przez producenta serwis.

b. chmura obliczeniowa (SW 4.4)

W przedmiotowym projekcie zakłada się zastosowanie rozwiązania mieszanego chmury hybrydowej. Wykonawca w analizie przedwdrożeniowej ma za zadanie zaproponować a później wdrożyć chmurę hybrydową opierając się o poniższe minimalne wskazania i parametry. Świadczenie usług on-line będzie miało miejsce w oparciu o zewnętrzne zasoby w modelu IAAS – infrastruktura dzierżawiona, natomiast zasilanie systemu danymi oraz ich przetwarzanie i przechowywanie będzie odbywało się w oparciu o zasoby lokalne z wykorzystaniem lokalnego repozytorium danych. Rozwiązanie takie zapewni optymalizację wykorzystania infrastruktury przetwarzania danych. Ważnym czynnikiem rzutującym na zastosowane rozwiązania są wymogi prawne. W chwili obecnej dokumentacja medyczna musi być archiwizowana i przechowywana w miejscu jej powstania. Stąd koniecznym jest, i takie jest założenie w projekcie, wdrożenie systemu archiwizacji danych oraz polityki bezpieczeństwa lokalnie. Zarazem jednak system musi gwarantować również gotowość do korzystania z przyszłych zasobów archiwizacji danych budowanych na poziomie regionalnym. Wykonawca w ramach chmury obliczeniowej musi dostarczyć usługę odzyskiwania usług w przypadku awarii w chmurze. W przypadku awarii Zamawiający będzie uruchamiał wcześniej przygotowany plan odzyskiwania. Maszyny wirtualne z lokalizacji podstawowej odtworzą się w zapasowej serwerowni lub w chmurze zewnętrznej. Po odtworzeniu, pracownicy Zamawiającego mają zostać przełączeni na ośrodek zapasowy i dalsza ich praca będzie kontynuowana online. Po naprawieniu awarii systemu muszą powrócić automatycznie do lokalnych ośrodków obliczeniowych.

Wykonawca w ramach chmury obliczeniowej dostarczy usługę uruchomienia zapasowego kontrolera domeny w chmurze zewnętrznej, który będzie umożliwiał użytkownikom systemów szpitala na zalogowanie się do sieci w przypadku awarii oraz udostępnienia usług SSO. Usługi w chmurze muszą być dostępne przez okres minimum 2 lat, a po tym okresie mogą zostać przedłużone lub skopiowane w obszar wirtualizacyjny maszyn Zamawiającego.

Minimalne wymagania do chmury obliczeniowej:

Lp.	Wymagania formalne
1.	<p>Chmura obliczeniowa SaaS musi spełniać wymagania określone w poniższych aktach prawnych:</p> <ul style="list-style-type: none"> Ustawa z dnia 24 stycznia 2012 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j. Dz.U. z 2012 r. poz. 159, dalej jako: „u.p.p.” lub „Ustawa o prawach pacjenta”); Ustawa z dnia 9 października 2015 roku o zmianie ustawy o systemie informacji o ochronie zdrowia i niektórych innych ustaw (dalej jako: „Nowelizacja z dnia 9 października 2015 roku u.s.i.o.z. i niektórych innych ustaw”)².

	<ul style="list-style-type: none"> • Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. Nr 101, poz. 926 dalej jako: „Ustawa o ochronie danych osobowych” lub „u.o.d.o”); • Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2013 r. poz. 1422, dalej jako: „u.ś.u.d.e.” lub „Ustawa o świadczeniu usług drogą elektroniczną”) • Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne z dnia 7 grudnia 2012 r. (Dz.U. z 2013 r. poz. 235 t.j. dalej jako: „Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne”); • Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. z 2014 r. poz. 243, dalej jako: „Prawo telekomunikacyjne”); • Ustawa z dnia 20 maja 2010 r. o wyrobach medycznych (Dz.U. z 2015 r. poz. 876, dalej jako: „Ustawa o wyrobach medycznych”) • Rozporządzenie Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. z 2015 r. poz. 2069, dalej jako: „Rozporządzenie ws. dokumentacji medycznej”); • Rozporządzenie Ministra Zdrowia z dnia 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. 2010 r. Nr 252 poz. 1697 z późn. zm., dalej jako: „Rozporządzenie ws. dokumentacji medycznej z 2010 r.”); • Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. 2004 r. Nr 100, poz. 1024, dalej jako: „Rozporządzenie na podstawie art. 39a UODO”); • PWDL – podmiot wykonujący działalność leczniczą w rozumieniu Ustawy o działalności leczniczej. PWDL w rozumieniu u.d.l. są zarówno podmioty lecznicze (przedsiębiorcy – spółki prawa handlowego, jak i nieprzedsiębiorcy – jednostki budżetowe), jak i praktyki lekarskie oraz pielęgniarские (również indywidualne). PWDL są więc wszelkie dopuszczalne formy wykonywania działalności leczniczej, zgodnie z polskim prawem; • Grupa Robocza z Art. 29 – Grupa robocza ds. ochrony danych powołana na mocy art. 29 dyrektywy 95/46/WE przyjętej dnia 15 lutego 2007 roku; • Opinia 5/2012 Grupy Roboczej z art. 29 – Opinia 5/2012 Grupy Roboczej z art. 29 w sprawie przetwarzania danych w chmurze obliczeniowej, tzw. cloud computing, WP 196. Opinia stanowi wyraz wspólnych poglądów organów ochrony danych osobowych państw członkowskich z wszystkich krajów członkowskich Unii Europejskiej. Częścią Opinii 5/2012 Grupy Roboczej z art. 29 jest zbiór rekomendacji dotyczących zasad powierzenia przetwarzania danych w chmurze;
	Wymagania dotyczące bezpieczeństwa
2.	<p>Chmura obliczeniowa musi spełniać następujące normy bezpieczeństwa:</p> <ul style="list-style-type: none"> • PN-ISO/IEC 27001 • PN-ISO/IEC 27002 • PN-ISO/IEC 27018 • HITRUST CSF <p>Do umowy należy dołączyć certyfikaty potwierdzające spełnianie powyższych norm.</p>
	Wymagania funkcjonalne
3.	<p>Chmura obliczeniowa opisana w pkt 4.4 musi być oparta o powszechnie dostępną przez Internet platformowy usługi hostowanej typu COTS (Commercial Of-The-Shelf) polegającą na udostępnieniu skalowalnej platformy pozwalającej wykorzystać w formie usługi serwerowe</p>



	<p>systemy operacyjne, silniki baz danych relacyjnych oraz inne aplikacje w środowiskach zwirtualizowanych.</p> <p>Usługa ta powinna się cechować następującymi parametrami:</p> <ol style="list-style-type: none"> 1. Gwarantowana umownie dostępność usługi na poziomie 99,00 %, 2. Możliwość skalowania usługi z przewidywalnymi kosztami takiego skalowania, 3. Automatyczna, nie wpływająca na ciągłość pracy systemu instalacja poprawek dla składników usługi, 4. Dostępność na żądanie wyników aktualnych audytów, w tym audytów bezpieczeństwa, dla usług i centrów przetwarzania danych oferujących te usługi, 5. Zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/składowanych w usłudze danych po stronie Zamawiającego, 6. Dostępność mechanizmów monitorowania zachowań użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych Zamawiającego, 7. Zawarcie w umowie na wykorzystanie zamawianej usługi tzw. Klauzul Umownych opublikowanych przez Komisję Europejską w zakresie ochrony danych osobowych, 8. Możliwość zastrzeżenia miejsca przetwarzania/składowania danych w usłudze do terytorium krajów Unii Europejskiej. 9. Dynamiczne zwiększanie i zmniejszanie zasobów sprzętowych bez przestoju w pracy dotychczasowego środowiska. 10. Wdrożenie nowej wersji aplikacji bez przestoju w pracy dotychczasowego środowiska. 11. Automatyczna, niewpływająca na ciągłość pracy systemu instalacja poprawek udostępnianych przez dostawcę systemu operacyjnego. 12. Możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową, pozwalającego na zachowanie jednolitej adresacji IP 13. Możliwość uruchomienia aplikacji internetowych wykorzystujących technologię ASP.NET z automatyczną dystrybucją ruchu sieciowego HTTP pomiędzy kilka pracujących serwerów. 14. Zarządzanie za pomocą graficznego interfejsu użytkownika oraz skryptów z możliwością zdalnego dostępu. 15. Możliwość przechowywania danych spełniająca następujące wymagania (opcjonalnie dostępnych w ramach usługi): <ol style="list-style-type: none"> a. Wysoka skalowalność, auto-partycjonowanie, load-balancing b. Obsługa przechowywania danych udostępnianych jako blob, tablica, dysk, plik, kolejka c. Wsparcie dla systemów klienckich Windows i Linux d. Skalowalność pojedynczego zasobu pamięci 500TB e. Szybkość dostępu do zasobu min 5GB/sek f. Replikacja danych - min. 3 kopie w ramach pojedynczej lokalizacji g. Replikacja do innej lokalizacji oddalonej o min 500km od lokalizacji podstawowej h. Udostępnienie zasobów pamięci poprzez REST API i. Gotowe biblioteki programistyczne środowisk programowania: .NET, Java/Android, Node.js, PHP, Ruby, Python, PowerShell
--	--

c. oprogramowanie użytkowe (SW 5.4.1.3);

System będzie odpowiadał za efektywne i bezpieczne tworzenie, przetwarzanie, gromadzenie oraz dystrybucję całości informacji medycznych związanych z przebiegiem leczenia pacjenta; od chwili przybycia do placówki medycznej aż do zakończenia procesu leczenia.

Będzie wspomagał lekarza w ocenie stanu zdrowia pacjenta, ułatwiał dostęp do pełnej dokumentacji medycznej pacjenta - bieżącej i archiwalnej, umożliwi wydruki wszystkich formularzy stosowanych w danej jednostce medycznej oraz zapewni obowiązkową sprawozdawczość rozliczeniową i statystyczną. Umożliwi elektroniczną komunikację w zakresie kierowania pacjenta do innych jednostek organizacyjnych zakładu (zlecenia) i odbioru wyników zleconych świadczeń. Umożliwi ponadto wykorzystanie Internetu do rejestracji pacjentów indywidualnych oraz realizacji usług zleconych przez kontrahentów zakładu. W zasadniczy sposób usprawni organizację procesu leczenia.

W ramach projektu pacjentom zostanie udostępniony interaktywny portal internetowy e-Pacjent stanowiący platformę elektroniczną świadczenia e-usług przedstawionych szczegółowo w pkt 4.2 Studium Wykonalności.

Po zakończeniu realizacji projektu w placówce usprawnione zostaną procedury rejestracyjne pacjentów do lekarzy. Za pomocą wiadomości e-mail lub wiadomości tekstowej SMS otrzymają potwierdzenie wybranego terminu, a w razie nieplanowanej absencji personelu medycznego powiadomienie o odwołaniu bądź przesunięciu terminu wizyty.

W każdej chwili pacjent będzie miał możliwość wglądu do swojej historii choroby (Elektroniczna Dokumentacja Medyczna). Po zalogowaniu w systemie będzie mógł przeglądać wszystkie wizyty, zalecenia, recepty i wyniki badań, np. celem przekazania informacji innemu lekarzowi albo opiekunowi, w przypadku osoby starszej lub dziecka.

W wyniku realizacji projektu personel Szpitala jak również pacjenci będą mieli dostęp do platformy e-usług za pomocą urządzeń przenośnych, takich jak laptop czy tablet. Powyższe rozwiązania mają na celu przeciwdziałanie zjawisku tzw. wykluczenia cyfrowego, w tym przypadku mogącego występować wśród pacjentów Szpitala, korzystających z usług medycznych w trybie stacjonarnym.

Przygotowanie do komunikacji z platformą P1

Systemy usługodawców, w tym Szpital przetwarzające elektroniczną dokumentację medyczną będą musiały komunikować się w przyszłości z powstającym Systemem Informacji Medycznej - SIM (dalej nazywanym platformą P1) administrowanym przez Ministra Zdrowia w celu realizacji zadań stawianych przez ustawę, o czym mówi m.in. art. 11 tej ustawy:

1. Usługodawcy prowadzą elektroniczną dokumentację medyczną.
2. Usługodawca za pośrednictwem SIM może uzyskać dostęp do danych, w tym danych osobowych i jednostkowych danych medycznych, zawartych w elektronicznej dokumentacji medycznej usługobiorcy, zgromadzonych w systemie teleinformatycznym innego usługodawcy, jeżeli jest to niezbędne do zapewnienia ciągłości leczenia lub prowadzonego postępowania diagnostycznego.
3. Usługodawca zamieszcza w SIM dane umożliwiające pobranie danych zawartych w elektronicznej dokumentacji medycznej przez innego usługodawcę lub pobranie dokumentów elektronicznych niezbędnych do prowadzenia diagnostyki, zapewnienia ciągłości leczenia oraz zaopatrzenia usługobiorców w produkty lecznicze i wyroby medyczne.

W celu zapewnienia wymiany informacji pomiędzy usługodawcami platforma P1 będzie gromadzić informacje o zdarzeniach medycznych mających miejsce u poszczególnych usługodawców. W celu realizacji tej wymiany zostały wybrane standardy komunikacji, które sprawią, że proces ten będzie mógł przebiegać w sposób zunifikowany.

Platforma P1 wykorzystuje dwa główne profile IHE w celu komunikacji między systemami:

4. IHE XDS - wykorzystywany do wymiany informacji o dokumentach medycznych (rozszerzona o informacje o zdarzeniu medycznym, w ramach którego dokumentacja ta powstała),
5. IHE XDM - wykorzystywany do importu do P1 dokumentów z placówek likwidowanych,
6. HL7 CDA (wersja 3) - w zakresie transferu nieobrazowych danych medycznych.

Dlatego koniecznym wymogiem dla wdrażanego systemu Elektronicznej Dokumentacji Medycznej w zakresie komunikacji z platformą P1 będzie zaimplementowanie obsługi wymienionych profili. Ponadto wymagane jest by współpraca z platformą P1 odbywała się za pomocą wymiany komunikatów w postaci plików XML (standard XML Schema). Tym samym wdrażany system zapewni wsparcie dla standardu przesyłania komunikatów SOAP (w wersji co najmniej 1.1) z załącznikami. Natomiast do opisu struktury i semantyki serwisu sieciowego (web service) zostanie wykorzystany standard WSDL (w wersji co najmniej 1.X). System wdrażany u Zamawiającego ma być przystosowany do komunikowania się z P1.

Metody uwierzytelniania

W projekcie zakłada się, że do uwierzytelniania wykorzystywany będzie tylko profil zaufany ePUAP, stanowiący zestaw informacji identyfikujących i opisujących podmiot lub osobę będącą użytkownikiem konta na ePUAP, który został w wiarygodny sposób potwierdzony przez organ podmiotu określonego w ustawie o informatyzacji podmiotów realizujących zadania publiczne.

W założeniu ePUAP jest platformą, która ma zapewnić dostępność usług publicznych poprzez zwiększenie liczby podmiotów korzystających z usług publicznych za pomocą różnych kanałów dostępu.

i. system oprogramowania obszaru medycznego – „część biała” (SW 5.4.I.3.1);

Wykonawca rozbuduje system HIS użytkowany w szpitalu lub z nim zintegruje za pomocą HL7 o funkcjonalność umożliwiającą zdefiniowanie treści oraz parametrów powiadomień, które będą mogły być wysyłane w danym okresie czasu określonej grupie pacjentów za pośrednictwem sms lub email:

- funkcjonalność umożliwiającą zdefiniowanie i zapisanie treści powiadomienia wysyłanego do grupy pacjentów,
- możliwość zdefiniowania zapytania SQL pobierającego listę pacjentów, lista pacjentów i akcje powiadomień obsługiwane na dedykowanej w tym celu formatce.
- w ramach listy możliwość ręcznego wyboru z listy, pacjentów do których wysłane zostanie powiadomienie
- zapisanie w systemie informacji o zgodzie pacjenta na wysyłanie powiadomień
- Kanał komunikacji e-mail, sms – do wyboru przez operatora definiującego parametry powiadomienia
- możliwość określenia ram czasowych oraz częstotliwości wysłania powiadomienia

ii. system oprogramowania obszaru administracyjnego – „część szara” (SW 5.4.I.3.2);

1. Rozbudowa systemu

1. Wykonawca rozbuduje użytkowany w szpitalu system administracyjny ERP InfoMedica o dodatkowe funkcjonalności lub wdroży system równoważny i zintegruje go z systemem posiadanym przez Zamawiającego, wynikające z parametrów minimalnych opisanych poniżej:

Obszar	Treść wymagania minimalnego
	Rozbudowa funkcjonalności obszaru administracyjnego o funkcje elektronicznego Rozliczanie Kosztów Leczenia Pacjenta
Rozliczanie Kosztów Leczenia Pacjenta	System ma możliwość automatycznego pobierania danych o pacjencie, w zakresie zrealizowanych mu świadczeń, z aplikacji medycznych (Przychodnia, Ruch Chorych i Apteczka oddziałowa), w tym co najmniej:
Rozliczanie Kosztów Leczenia Pacjenta	osobodni,
Rozliczanie Kosztów Leczenia Pacjenta	procedury,
Rozliczanie Kosztów Leczenia Pacjenta	badania,
Rozliczanie Kosztów Leczenia Pacjenta	leki.
Rozliczanie Kosztów Leczenia Pacjenta	System ma możliwość wydruku kosztowej karty leczenia pacjenta, dającej możliwość wyceny pobytu pacjenta (wydruk, jako załącznik może być podstawą wystawienia faktury za pobyt pacjenta nieubezpieczonego) z wyszczególnieniem kosztów świadczeń i leków istotnych kosztowo oraz włączeniem kosztów pozostałych świadczeń do kosztów ogólnych pobytu:
Rozliczanie Kosztów Leczenia Pacjenta	w zakresie kosztów leków – na poziomie cen leków z konkretnej dostawy, w ramach której zrealizowano podania dla pacjenta (integracja z modułami Apteka, Apteczka oddziałowa),
Rozliczanie Kosztów Leczenia Pacjenta	w zakresie rzeczywistych kosztów świadczeń (z ostatniego miesiąca, dla którego taka wycena istnieje – integracja z modułem Koszty) .
Rozliczanie Kosztów Leczenia Pacjenta	System ma możliwość grupowania kosztowych kart leczenia pacjentów wg zdefiniowanych kryteriów i prowadzenia analiz ekonomicznych (np. wg jednostek chorobowych, produktów rozliczeniowych).
Rozliczanie Kosztów Leczenia Pacjenta	System ma możliwość definiowania wskaźników kosztowo-przychodowych w oparciu o predefiniowane funkcje dla:
Rozliczanie Kosztów Leczenia Pacjenta	pacjentów,
Rozliczanie Kosztów Leczenia Pacjenta	ośrodków powstawania kosztów,

Rozliczanie Kosztów Leczenia Pacjenta	jednostek chorobowych,
Rozliczanie Kosztów Leczenia Pacjenta	produktów kontraktowych.
Rozliczanie Kosztów Leczenia Pacjenta	System ma możliwość zestawienia przychodów i kosztów hospitalizacji na poziomie:
Rozliczanie Kosztów Leczenia Pacjenta	pojedynczego pacjenta,
Rozliczanie Kosztów Leczenia Pacjenta	kodu JGP,
Rozliczanie Kosztów Leczenia Pacjenta	produktu jednostkowego,
Rozliczanie Kosztów Leczenia Pacjenta	produktu kontraktowego,
Rozliczanie Kosztów Leczenia Pacjenta	rozpoznania głównego.
Rozliczanie Kosztów Leczenia Pacjenta	System ma możliwość zestawienia statystyk kosztów pobytów z podziałem na lekarzy prowadzących.
Rozliczanie Kosztów Leczenia Pacjenta	System ma możliwość szacunkowej kalkulacji dotychczasowych kosztów leczenia pacjenta, w trakcie trwania hospitalizacji, w oparciu o dane historyczne lub zdefiniowane cenniki (w przypadku braku danych historycznych).
Rozliczanie Kosztów Leczenia Pacjenta	System ma możliwość prezentacji kosztów zleceń do jednostek zewnętrznych wg przyjętych cen umownych z daną jednostką.
Rozliczanie Kosztów Leczenia Pacjenta	System ma możliwość porównania liczby osobodni, wynikającej z danych zaewidencjonowanych w systemie medycznym, z liczbą osobni przesłaną do modułu KKL z modułu Rachunek Kosztów.

- Wykonawca dostarczy, zainstaluje i skonfiguruje oprogramowanie do obsługi elektronicznego rozliczania kosztów i kosztów leczenia pacjentów.
- Wykonawca zintegruje dostarczone oprogramowanie z systemem administracyjnym HIS funkcjonującym w szpitalu, co najmniej w zakresie:

Treść wymagania minimalnego

Zakres wymiany danych z oprogramowaniem HIS
System powinien umożliwiać wymianę danych o ilości zleceń wewnętrznych
<ul style="list-style-type: none"> ilości wykonanych badań laboratoryjnych z systemu HIS ilości wykonanych badań diagnostycznych z systemu HIS
System powinien umożliwiać wymianę danych statystyki stycznych, co najmniej w zakresie:
<ul style="list-style-type: none"> Ilość pacjentów wypisanych/leczonych Ilość wykonanych procedur Liczba łóżek Ilość wykonanych wizyt Ilość wykonanych porad
System powinien umożliwiać wymianę danych o przychodach z Apteki, co najmniej w zakresie:
<ul style="list-style-type: none"> dane wartościowe dotyczące przychodów leków na poszczególne magazyny dane o rozrachunkach wynikających z tych przychodów
System powinien umożliwiać wymianę danych o rozchodach z Apteki, co najmniej w zakresie:
<ul style="list-style-type: none"> dane wartościowe dotyczące rozchodów materiałów na poszczególne OPK w podziale na koszty szczegółowe
System powinien umożliwiać wymianę danych o lekach wraz z cenami, co najmniej w zakresie:
<ul style="list-style-type: none"> indeks materiałowy (nazwa leku, indeks, średnia cena, jednostka miary,
System powinien umożliwiać wymianę danych w zakresie obsługi faktur:
<ul style="list-style-type: none"> zapis danych o wystawionych dokumentach sprzedaży w systemie HIS wraz z rozrachunkami, dla nowo wystawianych faktur
System powinien umożliwiać przekazywanie danych kosztowych w zakresie:
<ul style="list-style-type: none"> koszty osobodni w podziale na OPK wartość wycenionych na dany miesiąc świadczeniach medycznych
System powinien umożliwiać wymianę danych o rozchodach z Apteczki Oddziałowej, co najmniej w zakresie:
<ul style="list-style-type: none"> Wartość podanych pacjentom leków z podziałem na Ośrodki Powstawania Kosztów

- Przeszkoli wskazaną grupę pracowników Zamawiającego w zakresie wykonywanych przez nich obowiązków służbowych.
- Przeszkoli administratorów w zakresie pozwalającym na samodzielne zarządzanie oprogramowaniem oraz budowę nowych procesów.
- Zamawiający posiada wymaganą do obsługi elektronicznego rozliczania kosztów licencję Koszty i Wycena Procedur Medycznych systemu ERP, w przypadku gdy Wykonawca zaproponuje swoje narzędzia elektronicznego rozliczania kosztów i kosztów leczenia pacjentów, Wykonawca dostarczy po jednej licencji dla każdego dostarczanego modułu.

iii. system wspomagania zarządzania – analizy BI (SW 5.4.I.3.3).

Nazwa/Opis wymagania minimalnego
<u>Grupa: Wymagania ogólne dotyczące architektury, logiki działania systemu, środowiska i warunków użytkowania dla kolektora danych</u>

<p>Wymaga się aby architektura systemu była zgodna z zasadami budowy rozwiązań klasy Business Intelligence, czyli aby system posiadał wydzielone repozytorium hurtowni danych, wydzielone repozytorium metadanych, warstwę analityczną, zasilanie danymi realizowane w oparciu o mechanizmy ETL</p>
<p>Wymaga się aby zasilanie hurtowni danych było realizowane poprzez udokumentowane interfejsy, a dokumentacja interfejsów będzie umożliwiała dostosowanie systemów źródłowych do wymagań wynikających z konieczności zasilenia hurtowni danych, także w takim wypadku, gdy producentem systemów źródłowych będzie inny podmiot niż dostawca systemu analiz zarządczych i controllingu. Zakłada się że definicja interfejsów będzie wskazywała między innymi na zakres wymaganych danych i sposób ich udostępnienia.</p>
<p>Wszystkie funkcje dostarczanego oprogramowania przeznaczone dla użytkowników końcowych mają być dostępne poprzez interfejs WWW. Dostęp przez przeglądarkę internetową nie może wymagać instalacji w przeglądarce internetowej żadnych dodatkowych wtyczek.</p>
<p>Dostarczone rozwiązanie ma już w pierwszej zainstalowanej wersji udostępniać standardowe grupy raportów obejmujące zakresy:</p> <ul style="list-style-type: none"> • finanse i księgowość, • analiza kosztów, • kontrola budżetu, • analiza danych z zakresu kadr i płac, • raportowanie w zakresie realizowanych kontraktów NFZ, • raporty z zakresu statystyki medycznej. <p>Zakres oczekiwanych raportów i analiz doprecyzowują dalsze wymagania w grupach definiujących wymagania funkcjonalne.</p>
<p>Poza wykorzystaniem wskazanych w wymaganiach standardowych raportów, użytkownik musi mieć możliwość definiowania własnych analiz opartych o dane gromadzone w hurtowni (w zakresie danych udostępnianych dla raportów standardowych).</p>
<p>Wymaga się aby system umożliwiał na poziomie warstwy analitycznej prezentowanie wyników analiz także w postaci graficznej np. w postaci wykresów adekwatnych do rodzaju prezentowanych danych.</p>
<p>Wymaga się aby na poziomie warstwy analitycznej system zapewniał możliwość drążenia danych w ramach powiązań występujących na poziomie modelu danych udostępnianych poprzez zdefiniowane raporty standardowe.</p>
<p><u>Grupa: Wymagania funkcjonalne dla zakresu – Finanse i Księgowość (Raporty standardowe)</u></p>
<p>Wymagany raport: Zestawienie aktywów i pasywów jednostki opieki zdrowotnej wg stanu na koniec wybranego miesiąca w danym roku, łącznie z możliwością wizualizacji stanów wszystkich pozycji na koniec więcej niż jednego miesiąca.</p>
<p>Wymagany raport: Prezentacja bilansu jednostki opieki zdrowotnej wg stanu na koniec wybranego miesiąca w danym roku łącznie z możliwością wizualizacji stanów wszystkich pozycji na koniec więcej niż jednego miesiąca.</p>
<p>Wymagany raport: Prezentacja zmian w kapitale własnym jednostki opieki zdrowotnej wg stanu na koniec wybranego miesiąca w danym roku.</p>
<p>Wymagany raport: Prezentacja rachunku wyniku w obydwu wariantach (porównawczym i kalkulacyjnym) wg stanu na koniec wybranego miesiąca w danym roku, łącznie z możliwością wizualizacji stanów wszystkich pozycji na koniec więcej niż jednego miesiąca.</p>

Wymagany raport: Prezentacja przepływów pieniężnych dla metody pośredniej wg stanu na dany rok.
Wymagany raport: Zestawienie zobowiązań i należności jednostki opieki zdrowotnej wg stanu na koniec wybranego miesiąca w danym roku, z możliwością wizualizacji wszystkich pozycji na koniec więcej niż jednego miesiąca.
Wymagany raport: Zestawienie przychodów jednostki opieki zdrowotnej wg stanu na koniec wybranego miesiąca w danym roku z możliwością wizualizacji wszystkich pozycji na koniec więcej niż jednego miesiąca.
Wymagany raport: Wykaz stanów kont (saldo, obroty, BO, persaldo) jednostki opieki zdrowotnej wg stanu na koniec wybranego miesiąca w danym roku.
Wymagany raport: Prezentacja wartości wskaźników rentowności wg stanu na koniec wybranego miesiąca w danym roku. Prezentowane wskaźniki: rentowność majątku, kapitału własnego, rentowność sprzedaży netto, rentowność działalności operacyjnej, rentowność netto, rentowność zasobów osobowych.
Wymagany raport: Prezentacja w postaci wykresu obejmującego dany rok miesięcznych wartości wskaźników rentowności.
Wymagany raport: Prezentacja wartości wskaźników płynności finansowej wg stanu na koniec wybranego miesiąca w danym roku. Prezentowane wskaźniki: wskaźnik płynności bieżącej, wskaźnik płynności szybkiej, wskaźnik płynności natychmiastowej, wskaźnik handlowej zdolności kredytowej.
Wymagany raport: Prezentacja w postaci wykresu obejmującego dany rok miesięcznych wartości wskaźników płynności finansowej.
Wymagany raport: Prezentacja wartości wskaźników analizy poziomej i pionowej wg stanu na koniec wybranego miesiąca w danym roku. Prezentowane wskaźniki: złota reguła bilansowa, złota reguła bilansowa II, złota reguła finansowania.
Wymagany raport: Prezentacja w postaci wykresu obejmującego dany rok miesięcznych wartości wskaźników analizy poziomej i pionowej.
Wymagany raport: Prezentacja wartości wskaźników zadłużenia wg stanu na koniec wybranego miesiąca w danym roku. Prezentowane wskaźniki: wskaźnik ogólnego zadłużenia, wskaźnik zadłużenia długoterminowego, wskaźnik zadłużenia kapitału własnego.
Wymagany raport: Prezentacja w postaci wykresu obejmującego dany rok miesięcznych wartości wskaźników zadłużenia.
Wymagany raport: Prezentacja wartości wskaźników struktury kosztów wg stanu na koniec wybranego miesiąca w danym roku. Prezentowane wskaźniki: wskaźnik struktury kosztów I – amortyzacja, wskaźnik struktury kosztów II – zużycie materiałów, wskaźnik struktury kosztów III – zużycie leków, wskaźnik struktury kosztów IV – zużycie sprzętu jednorazowego, wskaźnik struktury kosztów V – zużycie odczynników chemicznych i materiałów diagnostycznych, wskaźnik struktury kosztów VI – zużycie energii, wskaźnik struktury kosztów VII – usługi obce, wskaźnik struktury kosztów VIII – podatki i opłaty, wskaźnik struktury kosztów IX – wynagrodzenie, składki ZUS, fundusz pracy.
Wymagany raport: Prezentacja w postaci wykresu obejmującego dany rok miesięcznych wartości wskaźników struktury kosztów.
Wymagany raport: Prezentacja wg stanu na koniec wybranego miesiąca w danym roku wartości następujących wskaźników: wskaźnik EBITDA, wskaźnik zastosowania kapitału własnego, wskaźnik zastosowania kapitału obcego, wskaźnik ogólnej sytuacji finansowej, wskaźnik poziomu kosztów.
Wymagany raport: Prezentacja w postaci wykresu obejmującego dany rok miesięcznych wartości następujących wskaźników: wskaźnik EBITDA, wskaźnik zastosowania kapitału własnego, wskaźnik zastosowania kapitału obcego, wskaźnik ogólnej sytuacji finansowej, wskaźnik poziomu kosztów.
Grupa: Wymagania funkcjonalne dla zakresu – Analiza Kosztów (Raporty standardowe)

Wymagany raport: Zestawienie kosztów bezpośrednich w podziale na rodzaje kosztów zdefiniowane w jednostce opieki zdrowotnej wg stanu na koniec wybranego miesiąca w danym roku, łącznie z możliwością wizualizacji stanów wszystkich pozycji na koniec więcej niż jednego miesiąca.
Wymagany raport: Zestawienie przychodów i kosztów MPK (miejsc powstawania kosztów) jednostki opieki zdrowotnej wg stanu na koniec wybranego miesiąca w danym roku.
Wymagany raport: Zestawienie dla danego MPK jednostki opieki zdrowotnej głównych pozycji kosztowych wg stanu na koniec wybranego miesiąca.
Wymagany raport: Zestawienie prezentujące informację o progach rentowności poszczególnych oddziałów szpitalnych (wyrażone w punktach kontraktowych NFZ) wraz z danymi dotyczącymi kosztów oraz planie / wykonaniu (punkty) kontraktu NFZ.
<u>Grupa: Wymagania funkcjonalne dla zakresu – Kontrola Budżetu (Raporty standardowe)</u>
Wymagany raport: Prezentacja planu i wykonania budżetu przez komórkę budżetową wg stanu na koniec wybranego miesiąca w danym roku, łącznie z możliwością wizualizacji danych za wybrany miesiąc lub narastająco.
Wymagany raport: Prezentacja prognozy wykonania całości budżetu przez komórkę budżetową na podstawie średniej z dotychczasowego wykonania budżetu.
<u>Grupa: Wymagania funkcjonalne dla zakresu – Kadry i Płace (Raporty standardowe)</u>
Wymagany raport: Zestawienie prezentujące informacje o liczbie pracowników w etatach oraz osobach, liczbie przyjęć i zwolnień, średniej liczbie etatów oraz osób w przekroju grup zawodowych.
Wymagany raport: Zestawienie prezentujące informacje o liczbie pracowników w etatach oraz osobach, liczbie przyjęć i zwolnień, średniej liczbie etatów oraz osób w przekroju ośrodków powstawania kosztów.
Wymagany raport: Zestawienie prezentujące informacje o nieobecnościach chorobowych pracowników w podziale na nieobecności krótkie (do 7 dni), średniej długości (powyżej 7 a krócej niż 30 dni) oraz długie (powyżej 30 dni).
Wymagany raport: Zestawienie prezentujące informacje o płacach pracowników z uwzględnieniem składników płacowych.
Wymagany raport: Zestawienie prezentujące informacje o stanie opieki pielęgniarskiej na wskazanym oddziale szpitalnym. Stan opieki wyrażony jako stosunek zapotrzebowania na opiekę pielęgniarską wynikającą z liczby / stanu hospitalizowanych pacjentów oraz faktycznej obsady pielęgniarskiej.
Wymagany raport: Zestawienie porównawcze prezentujące uśrednione (w skali miesiąca) informacje o stanie opieki pielęgniarskiej na wskazanych oddziałach szpitalnych. Stan opieki wyrażony jako stosunek zapotrzebowania na opiekę pielęgniarską wynikającą z liczby / stanu hospitalizowanych pacjentów oraz faktycznej obsady pielęgniarskiej.
<u>Grupa: Wymagania funkcjonalne dla zakresu – Realizacja Kontraktów NFZ (Raporty standardowe)</u>
Wymagany raport: Aktualny stan realizacji umów z NFZ zawartych w poszczególnych latach z możliwością prezentacji danych w dotyczących planu i wykonania w wartościach punktowych lub kwotowo, w przekroju na: miesiąc sprawozdawczy, umowę, komórkę organizacyjną, OPK.
Wymagany raport: Aktualny stan realizacji umów z NFZ zawartych w zakresie określonych rodzajów umów we wskazanym roku, w przekroju na rodzaje umów i poszczególne umowy.

Wymagany raport: Aktualny stan realizacji umowy z NFZ dla wskazanej komórki organizacyjnej z dokładnością do zakresu świadczeń i miesiąca sprawozdawczego, w przekroju na: umowę, zakres świadczeń, miesiąc sprawozdawczy.
Wymagany raport: Raport szczegółowy realizacji umowy z NFZ z dokładnością do wybranej pozycji planu umowy (identyfikowanej przez: zakres świadczeń, wyróżnik i miesiąc sprawozdawczy), w przekroju na: zakres świadczeń z wyróżnikiem, komórkę organizacyjną -miejsce udzielania świadczeń, miesiąc sprawozdawczy.
Wymagany raport: Stan realizacji bieżących umów z NFZ w porównaniu do realizacji umów dotyczących tego samego rodzaju świadczeń w analogicznym okresie w poprzednich latach. Na jednym raporcie możliwe jest porównanie aktualnych danych z danymi z jednego wskazanego roku.
Wymagany raport: Monitorowanie potwierdzeń rozliczeń poszczególnych umów z NFZ do poziomu zakresu świadczeń dla całego roku lub kolejnych miesięcy sprawozdawczych, w przekroju na: umowę, zakres świadczeń, miesiąc sprawozdawczy.
Wymagany raport: Wartość rozliczeń JGP w poszczególnych latach dla oddziałów.
Wymagany raport: Wartość rozliczeń JGP dla komórek organizacyjnych dla kolejnych miesięcy sprawozdawczych.
Wymagany raport: Wartość rozliczeń JGP dla komórki organizacyjnej z dokładnością do pozycji planu umowy - dla kolejnych miesięcy sprawozdawczych z rozbiciem na zakresy świadczeń z wyróżnikiem, i kody grup JGP.
Wymagany raport: Szczegóły rozliczeń JGP dla komórki organizacyjnej i miesiąca z dokładnością do umowy i pozycji planu umowy - dla miesiąca sprawozdawczego z rozbiciem na zakresy świadczeń i kody grup JGP.
Wymagany raport: Porównanie wartości rozliczeń JGP dla komórek organizacyjnych - Oddziałów - dla kolejnych miesięcy sprawozdawczych.
Grupa: Wymagania funkcjonalne dla zakresu – Statystyka Medyczna (Raporty standardowe)
Wymagany raport: Zestawienie prezentujące informacje statystyczne dla pobytów szpitalnych obejmujące dane: liczba pacjentów przyjętych, liczba pacjentów wypisanych, liczba pacjentów aktualnie hospitalizowanych, średni koszt pobytu (o ile takie dane są dostępne w systemach źródłowych), liczba osobodni, liczba łóżek, wykorzystanie łóżek, liczb etatów lekarskich, liczba etatów pielęgniarskich. Dane prezentowane powinny być w przekroju na: miesiąc, jednostkę organizacyjną – tu oddziały szpitalny, OPK.
Wymagany raport: zestawienie prezentujące informacje statystyczne dotyczące porad ambulatoryjnych obejmujące dane: liczba porad, średni koszt porady (o ile takie dane są dostępne w systemach źródłowych), w przekroju na: miesiąc sprawozdawczy, jednostkę organizacyjną – tu poradnie, OPK.
Wymagany raport: Zestawienie prezentujące informacje statystyczne dla procedur medycznych obejmujące dane: liczba wykonań i średni koszt procedury (o ile takie dane są dostępne w systemach źródłowych). Dane prezentowane powinny być w przekroju na: miesiąc sprawozdawczy, procedurę medyczną, jednostkę organizacyjną (oddziały, poradnie), OPK.
Wymagany raport: Zestawienie prezentujące informacje statystyczne dotyczące wykonanych badań obejmujące dane: liczba wykonanych badań i średni koszt badania (o ile takie dane o kosztach są dostępne w systemach źródłowych). Dane prezentowane powinny być w przekroju na: miesiąc sprawozdawczy, badanie, jednostkę organizacyjną (zakłada się, że będą to pracownie), OPK.

Wymagany raport: Zestawienie zaewidencjonowanych w systemie dziedzinowym (HIS) kart diagnostyki i leczenia onkologicznego (DILO), prezentowane dane wg. stanu na ostatni dzień miesiąca wskazanego przez użytkownika.
Wymagany raport: Zestawienie prezentujące spis zdawczo - odbiorczy historii chorób generowany na bazie zarejestrowanych w systemie dziedzinowym (HIS) przypadków medycznych (zakończone hospitalizacje, udzielone porady oraz przypadki odnotowane w księdze odmów oraz udzielonych porad ambulatoryjnych).
Wymagany raport: Zestawienie prezentujące informacje o powtarzających się hospitalizacjach tego samego pacjenta (rehospitalizacjach) wraz z liczbą dni, jakie minęły od poprzedniego pobytu w szpitalu.
Wymagany raport: Zestawienie prezentujące listę przeniesień pacjentów pomiędzy oddziałami szpitalnymi we wskazanym przez użytkownika okresie.
Wymagany raport: Zestawienie prezentujące informację dotyczącą liczby punktów (kontrakt NFZ) wypracowanych przez poszczególnych lekarzy w zakresie liczby udzielonych porad.
<u>Grupa: Wymagania funkcjonalne dla zakresu – Zestawienia przekrojowe (Raporty standardowe)</u>
Wymagany raport: Zestawienie prezentuje przekrojowe informacje na temat funkcjonowania komórek organizacyjnych szpitala w zakresie obejmującym takie obszary jak: kontraktowanie NFZ, kolejki, ruch chorych, przychody / koszty, z możliwością ręcznej korekty wartości wyliczonych przez System przez użytkownika.
<u>Grupa: Wymagania dotyczące sposobu zasilania hurtowni danymi, organizacji procesów ETL</u>
Zasilanie hurtowni realizowane jest automatycznie poprzez procesy ETL zgodnie z harmonogramem zasilania w oparciu o zdefiniowane interfejsy.
Harmonogram zasilania hurtowni podlega edycji i dostosowaniu do specyfiki systemów źródłowych.
Musi być możliwość zdefiniowania dla poszczególnych obszarów hurtowni różnych parametrów określających częstotliwość zasilania dla danego obszaru, zgodnie ze zmiennością danych w systemach źródłowych.
Wymagane jest aby uprawniony użytkownik systemu mógł uruchomić „ręcznie” poszczególne ścieżki zasilania ETL.
Wymagane jest aby zasilanie hurtowni danymi za wybrany okres mogło być powtarzane wielokrotnie bez konieczności dokonywania specjalnych operacji administracyjnych na poziomie bazy rejestrów hurtowni.
Definicje ścieżek ETL muszą być przechowywane w plikach w formacie XML lub repozytorium, w celu ułatwienia zarządzania i weryfikowania na poziomie administratora systemu.
Repozytorium ETL może być rozmieszczone na dowolnej relacyjnej bazie danych.
W ramach dostarczanego systemu musi być dostępne narzędzie do graficznej prezentacji i edycji ścieżek ETL
Narzędzie do tworzenia ścieżek ETL musi umożliwiać podgląd struktur danych i zawartości danych po stronie źródeł zasilających hurtownię danych.
Zastosowane rozwiązanie ETL musi umożliwiać pobieranie danych z dowolnych relacyjnych baz danych.
Zastosowane rozwiązanie ETL musi umożliwiać pobieranie danych z baz „NoSQL” (np. Cassandra, MapR, MongoDB).
Zastosowane rozwiązanie ETL musi umożliwiać pobieranie danych z plików płaskich csv, arkuszy kalkulacyjnych, usług sieciowych, stron WWW,

Zastosowane rozwiązanie ETL musi umożliwiać pobieranie danych w formacie Json, HL7, LDIF, XML.
Zastosowane rozwiązanie ETL musi umożliwiać automatyczne tworzenie dokumentacji ścieżek ETL w formacie PDF, HTML, DOC, XLS
Zastosowane rozwiązanie ETL musi posiadać elastyczny/konfigurowalny mechanizm logowania z dokładnością do jednego przetwarzanego rekordu danych.
Zastosowane rozwiązanie ETL musi umożliwiać przenoszenie repozytorium definicji ścieżek ETL meta danych pomiędzy instalacjami poprzez funkcje eksportu i importu repozytorium.
Wymagane jest aby System dawał możliwość definiowania tzw. cyklicznych zasileń we wskazanych przez użytkownika interwałach (co najmniej: dziennie, tygodniowo, miesięcznie).
<u>Grupa: Wymagania dotyczące zarządzania metadanymi i translacji danych importowanych do hurtowni</u>
Rozwiązanie ma zawierać narzędzie, które umożliwia zarządzanie słownikami hierarchicznymi opisującymi dane biznesowe w ramach repozytorium metadanych (zarządzanie wymiarami).
Budowane słowniki w ramach repozytorium metadanych powinny mieć znaczniki czasowe określające, która z wersji hierarchii obowiązuje w danym okresie czasowym.
Rozwiązanie powinno zawierać wyodrębniony słownik translacji, umożliwiający zarządzanie regułami przetwarzania danych źródłowych na dane biznesowe reprezentowane w modelu logicznym hurtowni (przetworzenie danych źródłowych na pojęcia biznesowe).
W szczególności rozwiązanie powinno zapewniać możliwość takiej współpracy z źródłami udostępniającymi dane z zakresu finansów i księgowości, aby okresowe zmiany w zakładowym planie kont w źródłowym systemie F-K nie wymagały modyfikacji indywidualnych raportów bazujących na hurtowni danych, a jedynie jednokrotnej zmiany konfiguracji globalnej rozwiązania.
<u>Grupa: Wymagania dotyczące zarządzania prawami dostępu do informacji i bezpieczeństwa danych</u>
Wymaga się aby dostęp do systemu był możliwy tylko po uwierzytelnieniu użytkownika.
Wymaga się aby dostęp użytkownika do systemu był ograniczony przez rolę jaką użytkownik ma przyznaną w systemie.
Wymaga się aby system gromadził informacje o źródle, z którego pochodzą dane.
Wymaga się aby system gromadził informacje o wszystkich dostęпах do danych przetwarzanych na poziomie hurtowni.
Wymaga się aby system gromadził informacje dokumentujące wykonanie poszczególnych ścieżek ETL.

Ad 5. Wdrożenie e-usług (HRF II.5)

a. e – Rejestracja

Ze względu, iż Zamawiający posiada już wdrożoną podstawową funkcjonalność systemu e-rejestracja, zakres rozbudowy tego systemu obejmie aktualizację posiadanego przez Zamawiającego modułu e-Rejestracja do wersji technologicznej spełniającej warunki WCAG 2.0 i umożliwiającej obsługę portalu przez osoby niedowidzące. Przedmiotem zamówienia w tym zakresie, będzie też dokonanie analizy

celem dostosowania parametrów i funkcjonalności wdrożonego oprogramowania e-usług (projekt Mazowieckie e-zdrowie) do wymogów CSIOZ, bez ich powielania oraz wykonania Interfejsów zgodnie z Załącznikiem nr 4 do OPZ – Instrukcja stosowania Polskiej implementacji krajowej HL7 CDA. Wykonawca musi we wdrożeniu uwzględnić w szczególności zakres integracji z innymi modułami systemu e-usług oraz EDM oraz możliwością podpisywania się za pomocą e-puap (eIDAS).

b. e – Zgoda

System e-usług musi umożliwić wypełnienie i wydruk formularza e-zgody ze strony Internetowej oraz:

- System umożliwia wygenerowanie elektronicznego dokumentu e-Zgody i jego podpisanie w systemie ePUAP.
 - System umożliwia wyszukanie i pobranie zarejestrowanej e-Zgody z systemu EDM.
- System musi być zintegrowany z e-PUAP oraz e-IDAS.

c. e – Dokumentacja

Celem funkcjonalności jest usprawnienie udostępniania pacjentom dokumentacji medycznej przetwarzanej w jednostce ochrony zdrowia.

1. Prezentacja informacji o udzielonych świadczeniach opieki zdrowotnej oraz wpisach do list oczekujących (moje świadczenia):
 - 1.1. system prezentuje informacje o udzielonych świadczeniach opieki zdrowotnej – pobytach na oddziałach szpitalnych, udzielonych poradach wykonanych badaniach,
 - 1.2. system udostępnia obrazy diagnostyczne wykonane w Zakładzie Diagnostyki Obrazowej,
 - 1.3. system udostępnia wyniki badań laboratoryjnych wykonanych w jednostce,
 - 1.4. system prezentuje informacje o wpisach pacjentów na listach oczekujących.
2. Płatności on-line za udzielone świadczenia medyczne (moje płatności):
 - 2.1. system prezentuje informacje o wystawionych dokumentach sprzedaży dotyczących udzielonych świadczeń medycznych w postaci: data udzielenia świadczenia, nazwa świadczenia, nr dokumentu sprzedaży, kwotę do zapłaty, status płatności (opłacona/nieopłacona),
 - 2.2. system umożliwia zrealizowanie płatności on-line za udzielone świadczenie.
3. Rejestracja wniosku o udostępnienie dokumentacji medycznej:
 - 3.1. system umożliwia pacjentom rejestrację wniosków o udostępnienie dokumentacji medycznej. Wniosek obejmuje:
 - 3.1.1. dane osoby wnioskującej (właściciela konta w MPI): imię, nazwisko, dane identyfikacyjne (nr identyfikacyjny – w Polsce PESEL, lub nr dokumentu tożsamości),
 - 3.1.2. dane pacjenta (osoby wnioskującej lub jego autoryzowanego podopiecznego), którego dotyczy zamawiana dokumentacja medyczna,
 - 3.1.3. dat i specjalności komórki organizacyjnej pobytu, w czasie którego utworzono dokumentację medyczną pacjenta,
 - 3.1.4. formy udostępnienia dokumentacji medycznej (papierowa, elektroniczna na nośniku danych, elektroniczna do pobrania na portalu),
 - 3.2. system umożliwia przegląd informacji o świadczeniach medycznych udzielonych pacjentom w jednostce ochrony zdrowia oraz automatyczne przygotowanie wniosku udostępnienia dokumentacji medycznej dotyczącej wskazanego, zrealizowanego świadczenia medycznego.
 - 3.3. system umożliwia przegląd zarejestrowanych w Repozytorium EDM elektronicznych dokumentów medycznych związanych ze zrealizowanym świadczeniem medycznym (pobytem,

- poradą, badaniem) oraz automatyczne wygenerowanie wniosku o udostępnienie elektronicznej dokumentacji medycznej.
- 3.4. system rejestruje wniosek o udostępnienie dokumentacji medycznej w systemie Elektronicznego Obiegu Dokumentacji (EOD).
 4. Informowanie o dostępności zamawianej dokumentacji medycznej.
 - 4.1. system wysyła informacje o dostępności zamówionej w postaci wniosku dokumentacji medycznej z wykorzystaniem wybranego kanału komunikacji (SMS, e-mail, wiadomość portalowa),
 - 4.2. system umożliwia uruchomienie w kontekście zrealizowanego wniosku medycznego poprzez kliknięcie w odnośnik zawarty w wiadomości e-mail z informacją o dostępności zamówionej dokumentacji.
 5. Udostępnienie zamówionej dokumentacji medycznej:
 - 5.1. system prezentuje informacje o stanie przetwarzania wniosku o udostępnienie dokumentacji medycznej,
 - 5.2. system umożliwia zrealizowanie płatności on-line dla zamówień dokumentacji medycznej papierowej lub na nośnikach danych,
 - 5.3. system umożliwia pobranie dokumentacji medycznej udostępnianej na portalu.
 6. Przegląd i pobranie wyników badań laboratoryjnych:
 - 6.1. system umożliwia przegląd zrealizowanych badań laboratoryjnych, możliwe jest filtrowanie badań wg dat realizacji oraz wyszukiwanie wg nazwy badania,
 - 6.2. system prezentuje wyniki wskazanych badań laboratoryjnych,
 - 6.3. system umożliwia pobranie elektronicznego dokumentu medycznego będącego wynikiem badań laboratoryjnych.
 7. Integracja z systemem HIS:
 - 7.1. system integruje się on-line z systemem HIS w zakresie pobierania informacji o udzielonych świadczeniach medycznych; system nie tworzy własnego, oddzielnego repozytorium danych medycznych,
 - 7.2. system integruje się on-line z Repozytorium Elektronicznej Dokumentacji Medycznej (Repozytorium EDM w systemie HIS) w zakresie pobierania informacji o dostępnej elektronicznej dokumentacji medycznej. System nie tworzy własnego, oddzielnego repozytorium metadanych dokumentów i dokumentów w postaci elektronicznej,
 - 7.3. system integruje się on-line z modułem rozliczeń komercyjnych w zakresie pobrania informacji o wystawionych dokumentach sprzedaży z uwzględnieniem aktualizacji statusu płatności po zrealizowaniu płatności internetowej.
 8. Integracja z systemem EOD DocuSafe:
 - 8.1. rejestracja wniosku o udostępnienie dokumentacji medycznej w EOD,
 - 8.2. pobieranie statusu sprawy przetwarzania wniosku.
 9. Integracja z Rejestrem Sprzedaży systemu finansowo-księgowego:
 - 9.1. system umożliwia zarejestrowanie w Rejestrze Sprzedaży systemu finansowo-księgowego dokumentu sprzedaży w czasie realizacji płatności on-line za udostępnienie dokumentacji medycznej w postaci papierowej lub na nośniku danych.

d. e – Kontrahent

Wymagania funkcjonalne Administracja

1. Rejestracja instytucji – jednostki ochrony zdrowia, będącej stroną w procesach telekonsultacji:

- a. określenie roli instytucji względem innych organizacji: konsultant dla wskazanych organizacji, instytucja konsultowana przez wskazane organizacje,
 - b. wskazanie personelu (lekarzy) – uczestników procesów telekonsultacji, reprezentujących daną instytucję z określeniem uprawnień (ról: prezydent, ekspert, kwalifikator) rejestrowanej osoby do realizacji określonych operacji w systemie w kontekście danej instytucji,
 - c. rejestracja danych dostępowych do użytkowanych w danej instytucji systemów informatycznych zintegrowanych z platformą telekonsultacji.
2. Rejestracja danych personelu – uczestników procesów telekonsultacji:
- a. rejestracja danych osobowych i kontaktowych personelu,
 - b. utworzenie użytkownika w Systemie Kontroli Dostępu dla rejestrowanej osoby lub przypisanie osoby do istniejącego użytkownika,
 - c. określenie uprawnień (ról) użytkownika powiązanego z rejestrowaną osobą w kontekście wskazanej instytucji reprezentowanej przez tą osobę,
 - d. wskazanie personelu (lekarzy), który może być reprezentowany przez rejestrowaną osobę (np. lekarze, w których imieniu system jest obsługiwany przez sekretarkę medyczną).

Telekonsultacje przypadków medycznych

1. Rejestracja danych przypadku medycznego w celu zdalnej konsultacji z ekspertem:
- a. rejestracja danych osobowych pacjenta, którego dotyczy przypadek medyczny,
 - b. rejestracja krótkiego opisu przypadku medycznego,
 - c. możliwość wskazania rozpoznań opisujących przypadek medyczny,
 - d. wskazanie instytucji konsultującej przypadek medyczny (w przypadku, gdy jednostka konsultowana powiązana jest z wieloma jednostkami konsultującymi),
 - e. automatyczne uzupełnianie danych rejestrowanego przypadku medycznego (dane pacjenta, rozpoznania) na podstawie informacji o pobytach pacjentów zarejestrowanych w zintegrowanych systemach dziedzinowych HIS,
 - f. możliwość rejestracji załączników do przypadku medycznego, możliwość rejestracji załączników dotyczących lub powiązanych z wcześniej zarejestrowanymi (np. nowa wersja załącznika, notatka dotycząca innego załącznika itp.) ; załączniki mogą mieć postać:
 - i. notatek tekstowych,
 - ii. wskazanych zbiorów danych (np. obrazów, dokumentów) zlokalizowanych na wskazanych nośnikach danych; dla zbiorów w standardowych formatach obsługiwanych przez przeglądarki (dokumenty html, obrazy, filmy) należy zapewnić podgląd ich postaci,
 - iii. obrazów radiologicznych w formacie DICOM; należy zapewnić możliwość automatycznego wyszukiwania i dołączania plików DICOM znajdujących się na wskazanym nośniku danych; możliwość podglądu zawartości dołączonych plików DICOM (do podglądu nie jest wymagana jakość diagnostyczna),
 - iv. dokumentów medycznych w formacie HL7 CDA; należy zapewnić możliwość integracji z użytkowanym Repozytorium EDM systemu HIS w celu wyszukiwania i pobierania załączanych dokumentów medycznych.
 - g. automatyczne uzupełnianie danych przypadku medycznego na podstawie meta danych znajdujących się we wskazanym pliku DICOM,
 - h. automatyczne uzupełnianie danych przypadku medycznego na podstawie danych odczytanych z nagłówka dokumentów medycznych w postaci HL7 CDA.

2. Planowanie telekonsultacji przypadku medycznego:

- a. możliwość zaakceptowania wskazanego przypadku medycznego do telekonsultacji przez instytucję konsultującą; automatyczna akceptacja przypadku medycznego w przypadku rozpoczęcia realizacji procesu telekonsultacji,
- b. możliwość zaplanowania telekonsultacji w formie audio lub wideokonferencji – wskazanie planowanej daty i godziny oraz uczestników telekonsultacji,
- c. możliwość anulowania wcześniej zaplanowanej telekonsultacji w formie audio lub wideokonferencji,
- d. możliwość przypisania przypadku medycznego wskazanym osobom reprezentującym instytucję konsultującą (ekspertom),
- e. możliwość odrzucenia wskazanego przypadku medycznego z procesu telekonsultacji ze wskazaniem przyczyny odrzucenia,
- f. możliwość anulowania wskazanego przypadku medycznego przez prezentera (przedstawiciela instytucji rejestrującej przypadki medyczne) z podaniem przyczyny anulowania telekonsultacji.

3. Realizacja telekonsultacji przypadku medycznego:

- a. możliwość przeglądu kompletnych informacji dotyczących przypadku medycznego; możliwość pobrania załączników i ich przeglądu z wykorzystaniem zewnętrznych narzędzi (np. przegląd obrazów DICOM z wykorzystaniem systemów radiologicznych zapewniających wymaganą dla diagnostyki jakość prezentacji),
- b. możliwość rejestracji załączników do przypadku medycznego przez ekspertów konsultujących przypadki medyczne (w formie analogicznej do rejestracji załączników dołączanych przez prezenterów przypadku medycznego),
- c. prowadzenie telekonsultacji zarejestrowanego przypadku medycznego w formie audio lub wideo konferencji,
- d. automatyczna rejestracja przypadku medycznego w przypadku rozpoczęcia audio lub wideokonferencji (telekonsultacje w trybie pilnym),
- e. zakończenie telekonsultacji przez eksperta z wprowadzeniem podsumowania konsultacji przypadku medycznego.

4. Wykonawca udostępni interfejs Partnerom Projektu oraz przeszkoli po jednej osobie od każdego Partnera.

Wiadomości i przypomnienia

1. Informowanie zainteresowanych uczestników procesu telekonsultacji o zdarzeniach w systemie w postaci komunikatów w systemie oraz zasubskrybowanych wiadomości e-mail lub SMS. System powinien informować o następujących zdarzeniach:

- a. zainteresowanych ekspertów o zarejestrowaniu, modyfikacji danych i anulowaniu przypadków medycznych do telekonsultacji,
- b. zainteresowanych prezenterów o zaakceptowaniu, odrzuceniu i zakończeniu konsultacji przypadków medycznych w procesie telekonsultacji,
- c. zainteresowanych ekspertów o przypisaniu do konsultowania danych przypadków medycznych,
- d. uczestników telekonsultacji w formie audio i wideo konferencji o zaplanowaniu i zbliżających się terminach zaplanowanych telekonsultacji.

Bezpieczeństwo i audyt działania systemu

1. Rejestracja historii zmian danych osobowych pacjentów i personelu medycznego ze wskazaniem użytkownika dokonującego modyfikacji danych.

2. Rejestracja historii zmian danych medycznych (informacje opisujące konsultowany przypadek medyczny) ze wskazaniem użytkownika dokonującego modyfikacji danych.
3. Możliwość rejestracji informacji opisujących przypadek medycznych w postaci wersji roboczych, widocznych tylko dla autora tych informacji.

Wymagania niefunkcjonalne

1. Niezależność systemu od platformy systemowej stacji klienckich.
2. Możliwość użytkowania systemu na urządzeniach mobilnych (tablety, telefony komórkowe).
3. Udostępnienie otwartego interfejsu (API telekonsultacji) w postaci usług sieciowych, umożliwiających integrację rozwiązania z dowolnymi systemami użytkowymi w Jednostce Ochrony Zdrowia.

Asynchroniczna transmisja dużych zbiorów danych pomiędzy serwerem a klientami platformy telekonsultacji.

e. e – Wywiad

System umożliwia rejestrację przez pacjentów odpowiedzi na pytania stanowiące wywiad lekarski. Wywiad jest rejestrowany w kontekście planowanej realizacji świadczenia medycznego.

1. Rejestracja wywiadu lekarskiego:
 - a. system umożliwia pacjentom wypełnienie wywiadu lekarskiego w kontekście planowanej usługi medycznej,
 - b. system weryfikuje kompletność zebranego wywiadu lekarskiego – poprzez kompletność rozumiane udzielenie odpowiedzi na wszystkie pytania jej wymagające,
 - c. system zapisuje wywiad lekarski w postaci dokumentu określonego typu w Repozytorium EDM,
 - d. system przesyła wiadomości z prośbą o uzupełnienie wywiadu lekarskiego w zadanym czasie przed planowaną datą udzielenia świadczenia,
 - e. system umożliwia pacjentowi modyfikację wywiadu lekarskiego; zmodyfikowany wywiad rejestrowany jest jako kolejna wersja dokumentu w Repozytorium EDM.
2. Integracja z systemem HIS

System umożliwia przeprowadzenie badań satysfakcji pacjentów poprzez udostępnienie ankiet związanych z udzielonymi świadczeniami medycznymi.

3. Wypełnienie ankiety przez pacjentów:
 - a. system przesyła pacjentom wiadomości z prośbą o wypełnienie ankiety; wiadomości przesyłane są z wykorzystaniem wybranego kanału komunikacyjnego (SMS, e-mail, wiadomość portalowa); system umożliwia uruchomienie w kontekście ankiety do wypełnienia poprzez kliknięcie odnośnika przesłanego w wiadomości e-mail,
 - b. system umożliwia pacjentom wypełnienie zdefiniowanej ankiety dotyczącej udzielonego świadczenia medycznego.
 - c. system umożliwia udostępnienie różnych ankiet dla określonych usług medycznych.

f. e – Kolejka

Przedmiotem zamówienia jest system kolejkowy: e-kolejka, usprawniający zarządzanie ruchem pacjenta w obiekcie poradni specjalistycznych i poradni diagnostycznych. Po przyjęciu do rejestracji pacjent

pobiera bilet z urządzenia (biletomatu) i oczekuje na wezwanie w kolejce do rejestracji. Bilet od tego momentu jest przypisany do pacjenta podczas całej wizyty i za jego pomocą będzie identyfikowany również w kolejkach do gabinetów. System ma posiadać aplikację dla lekarza rejestracji, dla lekarza (gabinet) oraz administratora systemu. Kolejki do gabinetów lekarzy prezentowane będą na ekranach małego i dużego formatu. System będzie umożliwiał także powiadamianie pacjentów o zbliżających się wizytach za pomocą modułu SMS.

Zamawiający w ramach realizacji zamówienia zapewni wykonanie:

- wszystkie urządzenia muszą mieć doprowadzone zasilanie,
- dla wyświetlaczy musi być zagwarantowany dostęp do sieci IP
- powinna być dostępna zaawansowana konfiguracja na poziomie sieć IP

Funkcjonalności

Dostarczany system kolejkowy powinien zapewnić min. funkcjonalności:

- Zarządzanie kolejkami
 - Dodawanie, usuwanie, blokowanie
 - Definiowanie czasu pracy
 - Definiowanie tekstów na bilecie
- Zarządzanie kontami użytkowników:
 - dodawanie, usuwanie, modyfikowanie nowych kont użytkowników
 - konta użytkowników zabezpieczone hasłem
 - przypisywanie roli użytkownikom systemu
 - lista użytkowników powinna zawierać co najmniej następujące informacje: nazwa użytkownika lub jego imię i nazwisko, identyfikator
 - administrator musi mieć możliwość zmiany/resetowania haseł użytkowników
- Zarządzanie pacjentami:
 - możliwe w rejestracji z poziomu lekarza,
 - podgląd listy oczekujących pacjentów (lista pacjentów prezentowana w sugerowanej kolejności),
 - wezwanie pacjenta (kolejnego lub wybranego pacjenta z kolejki),
 - możliwość odroczenia wezwania pacjenta o czas konfigurowany w module administratora,
- Zarządzanie ekranami
 - przypisywanie ekranów do właściwej kolejki (lub kolejek),
 - możliwość powiązania ekranu z konkretnym stanowiskiem w gabinecie,
 - definiowanie informacji wyświetlanej na ekranie (wybór elementów: nazwa jednostki, nazwa poradni, dane lekarza, numer obsługiwany, numer/numery kolejny/e)
- Zarządzanie drukarkami
 - w zależności od konfiguracji systemu, wymagana jest możliwość pominięcia biletomatu i wydruku biletu w rejestracji,
 - w przypadku pominięcia biletomatu, system ma wydrukować bilet w rejestracji na drukarce biletowej
 - możliwość uruchomienia funkcji drukowania biletu w rejestracji automatycznie, po wykryciu zarejestrowania pacjenta do właściwej poradni w systemie HIS (powinien być wydrukowany bilet przypisane do konkretnej wizyty pacjenta),

- system musi wspierać wydruki na drukarkach biletowych podłączonych do sieci LAN
- Zarządzanie biletomatami
 - przypisywanie biletomatu do określonego zakresu kolejek,
 - definiowanie informacji wyświetlanej na ekranie (wybór elementów: nazwa jednostki, nazwa poradni),
 - możliwość definiowania puli biletów dostępnych do wydania w ramach konkretnych kolejek.
- Przechowywanie danych (dotyczących struktury organizacyjnej, personelu, gabinetów) w bazie danych, integracja z systemem HIS:
 - wymiana informacji dot. zarejestrowanych pacjentów,
 - wymiana informacji dot. badań,
 - wymiana informacji dot. harmonogramu pracy poradni
- Możliwość konfiguracji wysyłania wiadomości SMS do pacjentów, którzy posiadają numer telefonu komórkowego zdefiniowany w systemie. Powiadomienia mogą być wysyłane m.in. w celu poinformowania pacjenta o zbliżającym się czasie wywołania w systemie kolejkowym (w przypadku długiego czasu oczekiwania, pacjent może się oddalić od miejsca wezwania – zostanie poinformowany SMSem w czasie określonym odpowiednim algorytmem).
- Gromadzenie informacji i statystyk dotyczących pracy poszczególnych poradni, gabinetów i lekarzy, w tym danych dotyczących czasów obsługi pacjenta, czasów oczekiwania pacjenta,

Obliczanie szacunkowych czasów oczekiwania na podstawie zgromadzonych danych statystycznych, z możliwością wprowadzenia tej informacji na bilet.

System wydawania biletów oraz ekrany systemu muszą być zintegrowane z e-Kioskiem.

Ekran poczekalni musi być zintegrowany z e-kioskiem, ekran gabinetu lekarskiego musi być wyświetlany na ekranie komputera lekarskiego.

Ekran poczekalni

(dedykowany dla prezentacji wielu kolejek)

Parametry minimalne:

- Rozmiar ekranu: min 40"
- Rozdzielczość: 1920x1080 pikseli
- Złącze LAN (złącze RJ45), wbudowana karta sieciowa WiFi
- Mocowanie dedykowane lub VESA
- Uchwyt ścienny zapewniający regulację kąta nachylenia 0-10 stopni w pionie i 160 w poziomie
- Ekran może być wspierany urządzeniem realizującym zadania komunikacji/prezentacji
- Co najmniej 2 lata gwarancji producenta

Ekran gabinetu/rejestracji

Urządzenia stanowią wyświetlacze dedykowane dla gabinetów, okien rejestracji itp.

Parametry minimalne:

- Przekątna ekranu w zakresie 19" - 22" (wymaga dostępność urządzeń z ekranami zarówno zbliżonych do dolnej jak i górnej granicy)
- Rozdzielczość nie mniejsza niż 1280x800 pikseli

- Montażu ścienny (obudowa do montażu ściennego, bez dostępu do kabli)
- Złącze LAN (złącze RJ45), wbudowana karta sieciowa WiFi
- Ekran może być wspierany urządzeniem realizującym zadania komunikacji/prezentacji
- Co najmniej 2 lata gwarancji producenta

Biletomat

Parametry minimalne:

- Jednostka sterująca: uniwersalny komputer przemysłowy
 - Monitor dotykowy: min. 36 cali
 - Rozdzielczość: 1920x1080 pikseli
 - Drukarka paragonowa: termiczna, szerokość papieru 58-80mm, obcinacz papieru + prezenter.
 - Złącze LAN (złącze RJ45), wbudowana karta sieciowa WiFi
 - Co najmniej 2 lata gwarancji producenta
- W zależności od zapotrzebowania możliwe warianty:
- montaż ścienny,
 - montaż wolnostojący,
 - wersja z elektrycznie regulowaną wysokością.

Drukarka

Drukarka dostępna w rejestracji, umożliwiająca wygenerowanie biletu dla pacjenta.

Parametry minimalne:

- rozdzielczość druku: min 180 dpi
- szerokość druku (rolki): 58-80mm
- automatyczne odcinanie wydruków (deklaracja producenta co najmniej 1,5 mln odcięć)
- komunikacja: USB, LAN lub WLAN
- czujnik i sygnalizacja kończącego się papieru

Papier do drukarki termicznej:

- Papier ciągły w rolkach o szerokości 70-80mm
- (decyduje wymiar szerokości maksymalny deklarowany przez producenta drukarki)
- Długość jednej rolki 80 mb
- Gramatura 40-60 g/m

g. e – Identyfikacja

Identyfikacja Pacjentów zostanie zapewniona na bazie danych systemu HIS do wszystkich e-Uслуг wystawionych na portalu oraz w e-kiosku zintegrowanym z biletomatem opisanym powyżej. System e-Identyfikacji zostanie oparty również o infrastrukturę identyfikacji, monitoringu i lokalizacji pacjenta opisaną w części infrastruktury OPZ.

h. e – Powiadomienie

Wiadomości i przypomnienia

1. Informowanie zainteresowanych uczestników procesu telekonsultacji o zdarzeniach w systemie w postaci komunikatów w systemie oraz zasubskrybowanych wiadomości e-mail lub SMS. System powinien informować o następujących zdarzeniach:
 - a. zainteresowanych ekspertów o zarejestrowaniu, modyfikacji danych i anulowaniu przypadków medycznych do telekonsultacji,
 - b. zainteresowanych prezenterów o zaakceptowaniu, odrzuceniu i zakończeniu konsultacji przypadków medycznych w procesie telekonsultacji,
 - c. zainteresowanych ekspertów o przypisaniu do konsultowania danych przypadków medycznych,
 - d. uczestników telekonsultacji w formie audio i video konferencji o zaplanowaniu i zbliżających się terminach zaplanowanych telekonsultacji.

i. e – Informacja

Funkcjonalność umożliwia określenie zbioru usług dostępnych w Medycznym Portalu Informacyjnym (MPI) oraz zdefiniowanie parametrów dostępności.

1. Definicja profilu jednostki:
 - a. system umożliwia zdefiniowanie danych Jednostki Opieki Zdrowotnej prezentowanych w systemie MPI, w tym:
 - i. danych organizacji: nazwa organizacji, nr REGON, NIP,
 - ii. danych teleadresowych: adres siedziby, telefon, e-mail, adres witryny internetowej jednostki,
 - b. rozwiązanie umożliwia zdefiniowanie zintegrowanych systemów klasy HIS oraz konfiguracji połączenia z tymi systemami poprzez określenie lokalizacji oczekiwanych usług.
2. Rejestracja danych dostępności:
 - a. system umożliwia zdefiniowanie dostępności usługi w MPI; dostępność określana jest przez wskazaną usługę medyczną i opcjonalnie jednostkę organizacyjną w której ta usługa jest udzielana oraz personel świadczący to świadczenie w zdefiniowanym przedziale czasu:
 - i. możliwe jest zdefiniowanie okresu dostępności w MPI w postaci bezwzględnego przedziału czasu od do,
 - ii. możliwe jest określenie względnego okresu dostępności w MPI, rozumianego jako interwał czasu od daty bieżącej (np. liczba miesięcy od daty bieżącej),
 - b. system umożliwia publikację zdefiniowanej dostępności na Portalu (po publikacji dostępność jest widoczna na portalu – prezentowane są planowane wizyty związane z daną dostępnością),
 - c. system umożliwia wskazanie dostępności jako wykorzystywanej w systemie e-Rejestracji (takie dostępności będą wykorzystywane w procesie rezerwacji terminów wizyt).
 - d. system umożliwia, z dokładnością do wybranej dostępności, zdefiniowanie parametrów rezerwacji terminów wizyt:
 - i. możliwość wyboru personelu udzielającego świadczeń (wybór możliwy, wymagany, niemożliwy),

- ii. wymagalność skierowania.
- 3. Przegląd i modyfikacja danych dostępności:
 - a. system umożliwia przegląd danych dostępności w strukturach hierarchicznych:
 - i. usługa, jednostka organizacyjna (miejsce udzielania usługi medycznej), personel udzielający usługę w miejscu realizacji,
 - ii. usługa, personel, jednostka organizacyjna,
 - iii. personel, usługa, jednostka organizacyjna,
 - iv. personel, jednostka organizacyjna, usługa,
 - v. jednostka organizacyjna, usługa, personel,
 - vi. jednostka organizacyjna, personel, usługa.
 - b. system umożliwia filtrowanie dostępności wg stanu: w przygotowaniu, opublikowana, do rezerwacji, usunięta.
- 4. Rejestracja danych usług prezentowanych w MPI:
 - a. system umożliwia zarejestrowanie danych usług medycznych, prezentowanych w systemie MPI, zawierających: nazwę usługi, opis usługi, opis warunków udzielenia usługi,
 - b. system umożliwia rejestrację danych usług na podstawie danych ze zintegrowanego systemu HIS, system zapewnia przekodowanie identyfikatorów usług.
- 5. Rejestracja danych miejsca udzielania usługi prezentowanych w MPI:
 - a. system umożliwia zarejestrowanie danych jednostek organizacyjnych, które są prezentowane w MPI, zawierających: nazwę jednostki, dla komórek organizacyjnych – identyfikator i specjalność komórki (odpowiednio część VII i VIII systemu kodów resortowych), opis jednostki, dane teleadresowe: adres, telefon, e-mail, adres www.
 - b. system umożliwia rejestrację danych jednostek organizacyjnych na podstawie danych ze zintegrowanego systemu HIS, system zapewnia przekodowanie identyfikatorów jednostek organizacyjnych.
- 6. Rejestracja danych personelu medycznego udzielającego usługi prezentowanych w MPI:
 - a. system umożliwia zarejestrowanie danych personelu udzielającego świadczeń zdrowotnych zawierających: tytuł naukowy, imiona, nazwisko, wykonywane zawody oraz numery prawa wykonywania zawodu,
 - b. system umożliwia rejestrację danych personelu medycznego na podstawie danych ze zintegrowanego systemu HIS, system zapewnia przekodowanie identyfikatorów personelu.

Definicja ankiet i kwestionariuszy

Funkcjonalność umożliwia zdefiniowanie ankiet i kwestionariuszy udostępnianych w procesie rezerwacji terminów wizyt w Medycznym Portalu Informacyjnym oraz w celu badania satysfakcji pacjentów z udzielonych świadczeń zdrowotnych.

- 1. Definiowanie ankiet satysfakcji klienta.
 - a. system umożliwia rejestrację nazwy i opisu ankiety,
 - b. system umożliwia zdefiniowanie sekcji ankiet, dla każdej sekcji możliwe jest podanie nazwy i opisu; dane sekcji prezentowane są jako rozdziały ankiety,
 - c. system umożliwia zdefiniowanie pytań w ramach wybranych sekcji ankiety; dla pytania określa się: treść i opis pytania, wymagalność udzielenia odpowiedzi, typ odpowiedzi (tekstowy, numeryczny, data),
 - d. system umożliwia zdefiniowanie pytań zamkniętych, dla których określa się dziedzinę odpowiedzi – zbiór wartości do wyboru; dla poszczególnych możliwych odpowiedzi określa się ich treść oraz opis/komentarz do odpowiedzi,

- e. system umożliwia publikację ankiety w MPI (tylko opublikowane ankiety są dostępne dla pacjentów w MPI),
 - f. system umożliwia powiązanie ankiety z wybranymi usługami medycznymi, których realizacja wiąże się z możliwością wypełnienia ankiety; system umożliwia określenie interwału czasu względem daty udzielenia świadczenia, kiedy możliwe jest wypełnienie ankiety,
2. Definiowanie kwestionariuszy wypełnianych w kontekście planowanych w MPI wizyt pacjentów.
- a. system umożliwia definiowanie kwestionariuszy wypełnianych w kontekście rezerwacji terminu wizyty w sposób analogiczny do definicji ankiet satysfakcji (pkt. 1 a-e),
 - b. system umożliwia powiązanie kwestionariusza z wybranymi usługami medycznymi; rezerwacje terminów wizyt związanych z udzieleniem tych usług będą zawierały możliwość wypełnienia zdefiniowanego kwestionariusza.

Ad 6. Usługi wdrożeniowe (HRF II.6)

Przygotowanie dokumentacji projektowej

W ramach procesu wdrożenia Wykonawca opracuje w porozumieniu z Zamawiającym Dokumentację, która będzie dostarczona w języku polskim w formie elektronicznej na odpowiednio oznaczonych nośnikach elektronicznych CD/DVD umożliwiających wydrukowanie całości lub jej części oraz w formie papierowej w 2 egzemplarzach.

Dokumentacja składa się z następujących zakresów:

1. Dokumentacja Analizy przedwdrożeniowej wraz ze szczegółowym Harmonogramem wdrożenia.

Analiza przedwdrożeniowa powinna opisywać potrzeby Zamawiającego w poszczególnych obszarach, strukturę organizacyjną i przebiegi procesów biznesowych w szpitalu, obieg wymiany informacji i dokumentów oraz organizację pracy na poszczególnych stanowiskach. Przegląd posiadanej przez Zamawiającego infrastruktury technicznej pod kątem koniecznych inwestycji związanych z wdrożeniem Systemu.

2. Dokumentacja Projektowa.

Dokumentacja projektowa, opisuje szczegółowe procesy obejmujące warstwę biznesową, logiczną i techniczną, na podstawie, których będzie budowany system.

3. Dokumentacja Powykonawcza.

Dokumentacja powykonawcza powinna zawierać w szczególności:

- Schematy infrastruktury sprzętowej wraz z połączeniami poszczególnych ich elementów.
- Wykaz elementów infrastruktury sprzętowej, oprogramowania niezbędnego do działania Systemu, w tym również serwerów baz danych, serwerów aplikacyjnych, itp.
- Instrukcje instalacji wszystkich elementów infrastruktury sprzętowej i oprogramowania niezbędnego do działania Systemu.

- Wykaz zalecanych parametrów oprogramowania niezbędnych do sprawnego działania Systemu.
- Wykaz konfiguracji Systemu, pozwalającej na samodzielne administrowanie Systemem przez Zamawiającego po dokonaniu Odbioru Końcowego.
- Opisy struktur bazy danych, opisy interfejsów międzymodułowych, opisy plików i/lub parametrów konfiguracyjnych i parametryzujących system, instrukcje instalacji, deinstalacji każdego z elementów systemu tak, aby przeprowadzenie tych czynności mogło zostać wykonane samodzielnie przez administratorów systemu Zamawiającego.

4. Dokumentacja Użytkowa.

Dokumentacja użytkowa zawiera dokumenty będące instrukcjami obsługi, które w przystępny sposób pokazują jak użytkownik i administrator ma się posłużyć Systemem i infrastrukturą sprzętową, aby obsłużyć procesy i funkcje, jakie System ERP może realizować. Dokumentacja użytkowa powinna zawierać podręczniki umożliwiające samodzielne korzystanie z dostarczonego Sprzętu i oprogramowania, w szczególności:

- Opis procesów biznesowych realizowanych przez System
- Dokładny opis funkcjonalny modułów.
- Opis formatek w poszczególnych modułach wraz z opisem ich przeznaczenia.
- Opis wszystkich funkcji dostępnych na pojedynczej formatce.
- Opis poruszania się pomiędzy formatkami.
- Procedury rozpoznawania przyczyny wystąpienia błędu.
- Sposób korzystania z systemu pomocy.
- Instrukcje instalacji, konfiguracji i administracji.
- Instrukcje postępowania w przypadkach szczególnych oraz awarii.
- Instrukcje odtworzenia systemu po awarii
- Instrukcje restartu systemu.
- Instrukcje tworzenia kopii bezpieczeństwa i odtwarzania danych z kopii.

W przypadku wprowadzenia zmian w systemie w trakcie trwania umowy Wykonawca zobowiązany jest do niezwłocznego dostarczenia w ciągu 30 dni od dnia wprowadzenia zmian zaktualizowanej dokumentacji zarówno użytkownika jak i administratora.

Testy

- W ramach tego zadania Wykonawca przygotowuje i przeprowadzi testy, celem, których jest weryfikacja czy wszystkie prace wykonane w trakcie budowania Systemy zostały wykonane prawidłowo i zgodnie z założeniami funkcjonalnymi i jakościowymi.
- Testy zostaną przeprowadzone przez Wykonawcę przy współudziale pracowników Zamawiającego ewentualnie wskazanych przez Zamawiającego osób i podmiotów zewnętrznych.

- Pozytywne zakończenie testów wraz z usunięciem wskazanych wad jest niezbędne, aby dla poszczególnych komponentów oraz Systemu dokonać odbiorów w ramach poszczególnych etapów oraz Odbioru Końcowego.
- Zamawiający wykona pod nadzorem Wykonawcy próby wykonania kopii bezpieczeństwa i odzyskania z kopii systemu zgodnie z przekazanymi przez Wykonawcę procedurami. Pozytywne przeprowadzenie tego testu jest warunkiem koniecznym do otrzymania przez Wykonawcę ostatecznego odbioru.

Odbiór końcowy

- Zadanie to ma na celu potwierdzenie wykonanych wszystkich zadań wynikających z Projektu, w tym odebrania wszystkich komponentów i etapów Projektu oraz dostarczenia wszystkich wymaganych w zamówieniu dokumentów.
- Potwierdzeniem Odbioru końcowego jest podpisany przez zamawiającego Protokół odbioru końcowego.
- Dokonanie Odbioru końcowego zakończy prace przy budowie Systemu i będzie podstawą do przekazania Systemu do użytkowania produkcyjnego.

Ad 7. Usługi informatyczne (HRF II.7)

a. analiza przedwdrożeniowa, projekt techniczny systemu (SW 5.4.I.5.1);

Wykonawca w trakcie dostawy elementów systemu, musi wykonać analizę przedwdrożeniową oraz projekt techniczny systemu w ramach wdrożenia EDM i e-Usług (HRF II 3-5). Zamawiający po akceptacji projektu, zezwoli na wdrażanie systemu. Systemu i środowiska serwerowego Wykonawca nie może wdrożyć bez akceptacji Zamawiającego.

b. instalacja, konfiguracja sieci komputerowej, środowiska serwerów, stacji roboczych (SW 5.4.I.5.1);

Sieć komputerowa musi zostać zainstalowana w zgodzie obecnie istniejącą siecią której projekt znajduje się w Załączniku nr 3 do OPZ.

Stacje robocze zostaną rozstawione przez Wykonawcę, stary sprzęt zostanie zdemontowany i zeskładowany w miejscu wyznaczonym przez Zamawiającego.

Serwery muszą zostać skonfigurowane w środowisku wirtualizacyjnym dostarczonym przez Wykonawcę. Zamawiający posiada na obecnych serwerach środowisko VMware vSphere Essential. Systemy te muszą zostać uzupełnione do wersji pozwalającej na utworzenie jednej infrastruktury centrum danych wraz z serwerami wdrażanymi. System musi zostać tak skonfigurowany aby serwery wirtualne istniejące w tej infrastrukturze mogły migrować automatycznie pomiędzy serwerami fizycznymi w zakresie całego

środowiska wirtualizacyjnego, oraz wszystkie mogły mieć dostęp do pełnej infrastruktury serwerowej starej i nowej serwerowni, w tym macierzy danych.

c. wdrożenie systemów oprogramowania, e-usług, szkolenia użytkowników (SW 5.4.I.5.1);

1. Podczas szkolenia użytkowników musi zostać przekazana niezbędna wiedza w zakresie poprawnego użytkowania wdrażanych systemów HIS/EDM i e-usług w obrębie poszczególnych modułów w zakresie funkcjonowania, obsługi, administrowania i utrzymania systemów.
2. Zakres szkoleń musi obejmować praktyczną obsługę wszystkich funkcjonalności systemów.
3. Szkolenia muszą być prowadzone przez wykwalifikowanych specjalistów Wykonawcy, posiadających niezbędną wiedzę fachową w zakresie tematyki szkoleń.
4. Szkolenia będą musiały być przeprowadzane w siedzibie Zamawiającego, na dokumentach i sprzęcie Zamawiającego.
5. Wykonawca zapewni realizację szkoleń użytkowników w wymiarze 240h dla części białej, 240h dla części szarej, 40h dla części EDM i e-usług oraz 24h dla administratorów. Szkolenia będą prowadzone w grupach maksymalnie do 10 użytkowników oraz do 4 administratorów. Sala szkoleniowa zostanie dostosowana przez Wykonawcę na terenie Zamawiającego. Zamawiający udostępni pokój niezbędny do przeprowadzenia szkoleń.

d. migracja danych do nowego systemu (SW 5.4.I.5.1);

Zamawiający posiada oprogramowanie dedykowane do pracy w środowisku Szpitala Asseco AMMS. 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 (DZ.U. 1994 Nr 24 poz. 83 z późn. zm.) 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 (Dz. U. Nr 128, poz. 1402 z późn. zm.), 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. Na potrzeby przeprowadzenia migracji danych Zamawiający umożliwi Wykonawcy dostęp do baz danych posiadanych systemów informatycznych, nada wskazany pracownikom Wykonawcy niezbędne uprawnienia do tego aby mogli zapoznać się ze strukturami tabel w bazach danych oraz przekazać Wykonawcy posiadane instrukcje obsługi. Wykonawca ponosi odpowiedzialność za ewentualne szkody, wyrządzone przez jego pracowników w trakcie prac integracyjnych.

Zamawiający wymaga aby w zakresie nowo wdrażanych systemów objętych niniejszym zamówieniem, Wykonawca przedstawił stosowny dokument, opisujący „Interfejs komunikacyjny” z systemami programowymi Wykonawcy, pozwalający na integrację bazy danych systemu z innymi systemami, będącymi w przyszłości instalowanymi w infrastrukturze Zamawiającego.

e. integracja systemu z obszarami dziedzinowymi: diagnostyka obrazowa, gospodarka lekami (SW 5.4.I.5.1);

Wykonawca zobowiązany jest do połączenia swojego systemu z systemem funkcjonującym u zamawiającego – Asseco AMMS i Infomedica. Komunikacja z systemem Zamawiającego będzie odbywać się poprzez protokoły komunikacji zawarte w załączniku nr 2 do OPZ. Ze względu na to iż, system Asseco AMMS został wdrożony w projekcie „e-Zdrowie dla Mazowsza” realizowanego w ramach partnerstwa 23 szpitali i Urzędu Marszałkowskiego Województwa Mazowieckiego, funkcjonujący system nie może w okresie trwałości ww. projektu zostać wymieniony na inny, to też nie uznaje się za równoważną ofertę, ofertę na system informatyczny zawierający wymianę systemu HIS zamiast integrację z obecnie funkcjonującym.

Warunki organizacyjne przeprowadzenia integracji:

1. Zamawiający oświadcza, iż zgodnie z wiążącą go umową licencyjną z twórcami posiadanych systemów informatycznych, nie jest w posiadaniu kodów źródłowych modułów tych systemów.
2. Zamawiający dopuszcza realizację integracji z wykorzystaniem mechanizmów niewymagających współpracy z dostawcami posiadanych przez Zamawiającego systemów. Wykonawca odpowiedzialny będzie takie przygotowanie mechanizmów wymiany danych, aby nie powodowały one zakłóceń w pracy posiadanych przez Zamawiającego systemów.
3. Zamawiający dopuszcza na podstawie art.75 ust.2 pkt 3 ustawy Prawo autorskie (Dz.U. 2006, nr 90, poz.631) - konieczność dokonania przez Wykonawcę dekompilacji modułów systemów, dotychczas wykorzystywanych przez Zamawiającego, poprzez zwielokrotnienie kodu lub tłumaczenie jego formy w rozumieniu art.74 ust.4 pkt 1 i 2 ustawy Prawo autorskie (Dz.U. 2006, nr 90, poz.631), jeżeli będzie to niezbędne do uzyskania informacji koniecznych do osiągnięcia współdziałania modułów tych systemów z ZSI dostarczonym w ramach realizacji zamówienia. Wykonawca będzie zobowiązany wykonać czynności dekompilacyjne na własny koszt i ryzyko, w pełnym koniecznym zakresie z zastrzeżeniem, że czynności te będą odnosiły się tylko do tych części modułów tych systemów, które będą niezbędne do osiągnięcia współdziałania tych modułów z ZSI dostarczonymi przez Wykonawcę, a uzyskane informacje nie będą:
 - 3.1. wykorzystane do innych celów niż osiągnięcie współdziałania niezależnie stworzonego programu komputerowego;
 - 3.2. przekazane innym osobom, chyba że jest to niezbędne do osiągnięcia współdziałania niezależnie stworzonego programu komputerowego;

- 3.3. wykorzystane do rozwijania, wytwarzania lub wprowadzania do obrotu programu komputerowego o istotnie podobnej formie wyrażenia lub do innych czynności naruszających prawa autorskie.
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.

Na prośbę Wykonawcy, Zamawiający umożliwi Wykonawcy dostęp do baz danych posiadanych systemów informatycznych, udzieli wsparcia Wykonawcy w dokonaniu integracji, poprzez nadanie wskazanym pracownikom Wykonawcy niezbędnych uprawnień do pracy w systemie oraz do zapoznania się ze strukturami tabel w bazach danych posiadanych systemów, a także przekaże Wykonawcy posiadane instrukcje obsługi. Wykonawca ponosi odpowiedzialność za ewentualne szkody, wyrządzone przez jego pracowników w trakcie prac integracyjnych.

W przypadku, gdy Wykonawca będzie chciał wykonać integrację z wykorzystaniem komercyjnych interfejsów, udostępnianych przez producentów posiadanych przez Zamawiającego systemów:

1. Uzyskanie opisów interfejsów lub innych sposobów wymiany danych do integracji z wymienionymi w SIWZ systemami oraz określenie wykonawcy lub wykonawców tych integracji jest obowiązkiem Wykonawcy,
2. Ustalenie kosztów integracji z systemami posiadanymi przez Zamawiającego jest obowiązkiem Wykonawcy,
3. Koszty integracji są częścią ceny, składanej przez Wykonawcę, oferty na Wdrożenie oprogramowania wspomagającego pracę komórek administracyjnych. Wykonawca zobowiązany jest uwzględnić w ofercie pełny koszt wykonania integracji uwzględniający również, o ile będzie to konieczne, wykonanie modyfikacji interfejsów wymiany danych posiadanych systemów oraz zakup niezbędnych do integracji licencji.

Zamawiający informuje, że oczekuje możliwości integracji w projektowanym systemie w zakresie danych wymaganych i opisanych na stronach Centrum Systemów Informacyjnych Ochrony Zdrowia w ramach integracji z systemami P1, P2 oraz P4: <https://www.csioz.gov.pl/edm/>

Natomiast w zakresie danych dotyczących szyny regionalnej (CASE), precyzuje wymagania dla dostawców systemów dziedzinowych do potrzeb związanych z możliwością zintegrowania z CASE w przyszłości:

- Wykonawca systemów dziedzinowych, które są integrowane z CASE ma za zadanie dostarczenie interfejsów lub aplikacji do generowania danych z systemu SSI i pozostałych (w szczególności ERP/ obieg dokumentów , e-usług itp.) wymaganych do BI.
- CASE sprawdza kompletność wprowadzonych danych przed ich przekazaniem do warstwy regionalnej.
- CASE ma możliwość przekazania danych niekompletnych.
- CASE zapewnia w warstwie regionalnej zapis danych przekazanych od podmiotów leczniczych z warstwy lokalnej.
- Przekazanie danych odbywać się w trybie on-line, lub poprzez import plików (formularzy, arkuszy) uzupełnionych kompletnymi danymi albo poprzez wypełnienie formularzy na stronie Web Case bezpośrednio przez użytkownika..
- Dane w warstwie lokalnej w szpitalu są gromadzone w predefiniowanych formularzach.

- Operacja wypełnienia predefiniowanych formularzy ma być inicjowana w lokalnym systemie źródłowym (SSI, ERP, Workflow, e- usługi) automatycznie.
- W jej wyniku ma zostać wyświetlony odpowiedni formularz wypełniony danymi z systemu źródłowego.
- Zestaw formularzy zostanie dostarczony przez Wykonawcę zgodnie z wymaganiami Zamawiającego dotyczącymi zakresu danych. Obecnie dostarczono ok 40 formularzy. Plik XML z wszystkimi wymaganiami dla integratora w załączeniu.
- CASE w części dotyczącej zasilania hurtowni danych komunikuje się za pomocą języka XML.”.

f. opieka powdrożeniowa, wsparcie użytkowników (SW 5.4.I.5.1);

Wykonawca zobowiązuje się do świadczenia usług gwarancyjnych przez okres 24 miesięcy (liczonych od momentu zakończenia projektu) dla całości oferowanego Systemu i Infrastruktury.

1. Klasyfikacja zmian oprogramowania w trakcie eksploatacji:
 - a) poprawki - to zmiany oprogramowania, naprawiające wady produktu, które ujawniły się po jego sprzedaniu. Wady te powodują, że program nie posiada gwarantowanych przez Wykonawcę funkcjonalności. Dokonywane w ramach gwarancji,
 - b) udoskonalenia - zmiany oprogramowania mające na celu poprawienie funkcjonalności, stabilności lub bezpieczeństwa użytkowania. Nie zmieniają cech podstawowych produktu, poprawiają jego funkcjonowanie, objęte realizowanym zamówieniem,
 - c) uaktualnienia - zmiany prowadzące do uaktualnienia wersji oprogramowania objęte realizowanym zamówieniem,
2. Klasyfikacja błędów:
 - a) błąd krytyczny (awaria) – oznacza zaprzestanie działania Systemu, wynikających z przyczyn, za które odpowiada Wykonawca
 - b) błąd niekrytyczny (usterka) – oznacza ograniczenie działania Systemu, wynikających z przyczyn, za które odpowiada Wykonawca
3. Wykonawca w ramach trwania gwarancji zobowiązany jest do utrzymywania gotowości do czynności serwisowych, przyjmowania zgłoszeń i podejmowania czynności serwisowych głównie poprzez łącza zdalne oraz w wymagających tego okolicznościach przyjazd do siedziby Zamawiającego.
4. Zamawiający wymaga, aby Wykonawca posiadał aplikację internetową do przyjmowania i obsługi zgłoszeń, będącej podstawą komunikacji między Zamawiającym i Wykonawcą w zakresie zgłoszeń. Aplikacja powinna posiadać możliwość wysyłania powiadomień na temat zgłoszeń na podany adres e-mail, możliwość generowania raportów związanych ze zgłoszeniami.
5. Wszelkie błędy będą zgłaszane przez Zamawiającego poprzez dedykowaną aplikację internetową w wyjątkowych sytuacjach drogą elektroniczną lub telefonicznie.
6. Wykonawca będzie zobowiązany do niezwłocznego potwierdzania otrzymanego zgłoszenia drogą elektroniczną.
7. W ramach usług gwarancyjnych Wykonawca zobowiązuje się usuwać wykryte lub powstałe awarie, usterki (błędy systemu) na swój koszt w terminie określonym w serwisie gwarancyjnym.
8. Wykonawca świadczyć będzie usługi serwisu gwarancyjnego na zasadach określonych poniżej.
9. W ramach gwarancji Zamawiający zobowiązany jest zgłaszać wykryte awarie, wady lub błędy Oprogramowania, a Wykonawca usuwać zgodnie z uzgodnioną procedurą zgłaszania awarii lub usterek.
10. Naprawy gwarancyjne odbywać się będą na poniższych zasadach i w określonych terminach:

10.1. Usuwanie awarii i usterek w oprogramowaniu (godziny robocze liczone w dniach roboczych)

- a) błąd krytyczny – oznacza zaprzestanie działania oprogramowania systemu
- dostęp zdalny (pierwszorzędnie) - czas reakcji: liczba godzin roboczych od momentu zgłoszenia do Wykonawcy, czas usunięcia błędu: liczba godzin roboczych od momentu przyjęcia zgłoszenia przez Wykonawcę

Błąd krytyczny	Część medyczna	Część administracyjna
Czas reakcji	8 h	12 h
Czas naprawy	24 h	24 h

- b) błąd niekrytyczny - oznacza ograniczenie działania oprogramowania ZSI
- dostęp zdalny (pierwszorzędnie) - czas reakcji: liczba godzin roboczych od momentu zgłoszenia do Wykonawcy, czas usunięcia błędu: liczba dni roboczych od momentu przyjęcia zgłoszenia przez Wykonawcę ;

Błąd niekrytyczny	Część medyczna	Część administracyjna
Czas reakcji	8 h	24 h
Czas naprawy	60 dni	60 dni

10.2. W przypadku wykazania awarii usterek (błędów) zgłoszonych do Wykonawcy przez Zamawiającego w internetowym systemie rozwiązywania problemów, Wykonawca wypełni swoje zobowiązanie gwarancyjne, w ramach struktur organizacji serwisowej Wykonawcy, albo poprzez dostarczenie Zamawiającemu, według wyboru Wykonawcy, Update'u lub Upgrade'u oprogramowania, lub też, - według wyboru Wykonawcy - poprzez usunięcie awarii lub usterek (błędów); usunięciem awarii lub usterek może być, między innymi, wskazanie stosownego, akceptowalnego sposobu uniknięcia skutków awarii lub usterek, które to działania muszą skutkować wyeliminowaniem awarii lub usterek. Zamawiający zapewni Wykonawcy pełne i bezpłatne wsparcie, w szczególności poprzez zapewnienie współpracy pracowników, zapewnienie pomieszczeń do pracy oraz możliwie najdokładniejszego opisu awarii lub usterek, dostarczając wymagane dane oraz tworząc połączenia telekomunikacyjne z serwerem bazy danych. Zamawiający zobowiązuje się do zaakceptowania każdej bezpłatnej nowej wersji oprogramowania.

10.3. Zgłaszanie awarii i usterek przez Zamawiającego:

- a) Zgłaszanie awarii i usterek przez Zamawiającego może następować w jednej z niżej wymienionych form:

- pierwszorzędnie poprzez dedykowaną witrynę internetową Wykonawcy,
- telefonicznie,
- pocztą elektroniczną.

Zgłoszenia awarii i usterek Zamawiający może wykonywać całodobowo z wyłączeniem zgłoszeń telefonicznych, które mogą się odbywać w godzinach od 8.00 – 16.00. Przyjmuje się, że w przypadku, gdy zgłoszenie zostanie wykonane w dni robocze po godzinie 16.00 lub w dni ustawowo wolne od pracy, będzie ono traktowane jako zgłoszenie dokonane w najbliższym dniu roboczym po dniu zgłoszenia;

- b) po usunięciu przez Wykonawcę awarii lub usterek, Wykonawca zobowiązany jest poinformować o tym niezwłocznie Zamawiającego. Dopuszcza się następujące formy przekazywania potwierdzenia o usunięciu awarii/usterek:

- wpis potwierdzający poprawność wykonanych zmian, dokonany przez Zamawiającego na dedykowanym portalu
 - pocztą elektroniczną na wskazany przez Zamawiającego adres poczty elektronicznej,
 - protokołem usunięcia awarii/usterki utworzonym w trakcie wizyty serwisanta Wykonawcy,
- c) potwierdzenie zakończenia prac naprawczych przez Wykonawcę może zostać wydane wyłącznie przez upoważnioną przez Zamawiającego osobę;
- 11. W ramach usług gwarancyjnych Wykonawca zapewnia Zamawiającemu:
 - 11.1. Dostarczanie nowych wersji oprogramowania uwzględniających:
 - a) Zmiany zachodzące w powszechnie obowiązujących przepisach prawa lub przepisach prawa wewnętrznego obowiązujących na podstawie delegacji ustawowej,
 - b) Zmiany związane z podniesieniem jakości i funkcjonalności oprogramowania lub usuwających wykryte przez Wykonawcę błędy w działaniu oprogramowania.
 - 11.2. Wykonawca zobowiązany jest informować o wszystkich nowych wersjach oprogramowania wraz z przedstawieniem wykazu dokonywanych zmian, na wskazany przez Zamawiającego adres poczty elektronicznej.
 - 11.3. Reakcję na zgłaszane przez Zamawiającego problemy.
 - 11.4. Analizę zgłoszonego problemu i jego usunięcie.
- 12. Na dzień podpisania Protokołu odbioru przedmiotu zamówienia, Wykonawca zapewni, że system działa poprawnie i jest zgodny z obowiązującymi przepisami prawa.
- 13. Gwarancja na oprogramowanie osób trzecich (oprogramowanie zewnętrzne) dostarczone przez Wykonawcę będzie świadczona zgodnie z warunkami zapewnianymi przez producenta tego oprogramowania z zastrzeżeniem warunków opisanych we wzorze umowy.
 - 13.1. Wykonawca zapewni dostępność do aktualizacji producentów dostarczonego oprogramowania systemowego, narzędziowego i motorów baz danych. Okres wsparcia dla tego oprogramowania rozpoczyna się z dniem podpisania przez Strony protokołu odbioru i trwa do dnia wygaśnięcia gwarancji na dostarczony System.
- 14. Warunki gwarancyjne dla sprzętu
 - a. Wykonawca gwarantuje, że dostarczony serwer jest wolny od wad prawnych oraz od wad fizycznych, produkcyjnych, bądź wynikających z jakiegokolwiek działania, lub zaniechania Wykonawcy,
 - b. Wykonawca udziela Zamawiającemu gwarancji na okres 36 miesięcy,
 - c. dostarczony sprzęt musi być fabrycznie nowy (rok produkcji 2016 lub nowszy),
 - d. gwarancja na dostarczony przez Wykonawcę sprzęt musi umożliwiać:
 - i. wykonywanie całej usługi naprawy w miejscu instalacji siedzibie Zamawiającego,
 - ii. zgłaszanie uszkodzeń 5 dni w tygodniu - w dni robocze
 - iii. czas naprawy nie dłuższy niż 4 dni robocze od momentu zgłoszenia awarii, w przypadku braku możliwości naprawy na miejscu, dostarczenie na koszt i ryzyko Wykonawcy urządzenia zastępczego o parametrach zgodnych z urządzeniem uszkodzonym, wraz z jego instalacją i konfiguracją do pracy w miejsce urządzenia uszkodzonego,
 - iv. w przypadku, gdy czas naprawy przekroczy 30 dni roboczych - wymianę uszkodzonego urządzenia na nowe o parametrach nie gorszych niż urządzenie uszkodzone, wraz z jego instalacją i konfiguracją do pracy w miejsce urządzenia uszkodzonego,
 - v. transport sprzętu do naprawy jak i naprawionego/wymienionego pomiędzy Zamawiającym a serwisem na swój koszt i ryzyko gwaranta,
 - e. ponadto w ramach gwarancji dla całego dostarczonego sprzętu:

- i. Zamawiający nie ma obowiązku przekazywania sprzętu do naprawy z oryginalnymi opakowaniami fabrycznymi,
- ii. okres gwarancji dla dostarczonego sprzętu i wszystkich podzespołów rozpoczyna się nie wcześniej niż z dniem jego odbioru przez Zamawiającego i podpisaniem przez obie Strony końcowego protokołu odbioru,
- iii. Wykonawca ma obowiązek zapewnienia nieodpłatnie sprzętu zastępczego na czas naprawy o parametrach nie gorszych wraz z konfiguracją i instalacją w miejsce sprzętu uszkodzonego; Zamawiający może każdorazowo zrezygnować z obowiązku dostawy sprzętu zastępczego na czas naprawy,
- f. w przypadku, gdy Wykonawca nie usunie wad w terminie określonym wyżej Zamawiający ma prawo do usunięcia wad we własnym zakresie lub powierzenia naprawy Urzędzień innemu podmiotowi na koszt i ryzyko Wykonawcy, bez utraty prawa do gwarancji udzielonej przez Wykonawcę,
- g. warunki gwarancji niewymienione powyżej będą realizowane zgodnie z zapisami gwarancji udzielanej przez producenta.

g. audyt bezpieczeństwa wdrożonego systemu na zgodność z wymogami przepisów (SW 5.4.I.5.1).

Wykonawca przeprowadzi audyt wdrożonych systemów za zgodność z wszystkimi zapisami Studium Wykonawalności Projektu.

5. Etapy projektu i termin realizacji

Etapy mogą być realizowane równolegle w celu optymalizacji procesu wdrożenia.

Każdy Etap projektu zakończony zostaje fakturą rozliczeniową.

- 1) Etap I – realizacja zadania wymienionego w HRF II.1, w terminie do 120 dni od daty podpisania Umowy,
- 2) Etap II – dostawa sprzętu wymienionego w HRF II.2, w terminie do 30 dni od daty podpisania Umowy,
- 3) Etap III – rozbudowa systemu wymienionego w HRF II.3 i w HRF II.5-7, w terminie do 60 dni od daty podpisania Umowy,
- 4) Etap IV – dostawa i usługi wymienione w HRF II.4, w terminie do 30 dni od daty podpisania Umowy,
- 5) Etap V – Testy i odbiór końcowy - do 20 dni od zakończenia etapów I – IV.

Spis załączników:

1. PFU
2. Protokoły komunikacji w systemie AMMS
3. Instrukcja stosowania Polskiej implementacji krajowej HL7 CDA w systemach EDM.
4. Studium Wykonalności Projektu