Załącznik nr 2 do SIWZ

Program funkcjonalno – użytkowy

Wykonanie projektu wraz z budową sieci informatycznej w budynkach Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Nowym Mieście nad Pilicą oraz dostawą, montażem, konfiguracją i uruchomieniem niezbędnego sprzętu serwerowego i komputerowego w ramach projektu „Wdrożenie usług E-zdrowie w SP ZOZ Nowe Miasto nad Pilicą”

Program funkcjonalno - użytkowy dotyczy obiektów budowlanych:

Samodzielny Publiczny Zakład Opieki Zdrowotnej w Nowym Mieście nad Pilicą
ul. Tomaszowska 43
26-420 Nowe Miasto nad Pilicą

Samodzielny Publiczny Zakład Opieki Zdrowotnej. Przychodnia Rejonowa w Drzewicy
ul. Stanowa 27
26-340 Drzewica

Samodzielny Publiczny Zakład Opieki Zdrowotnej. Ośrodek Zdrowia w Żdżarach
Żdzary 75C
26-420 Nowe Miasto nad Pilicą

CPV – 45315500-4 instalacyjne roboty elektryczne
CPV – 45314320-0 instalowanie okablowania komputerowego
CPV – 45331200-8 instalowanie wentylacji i klimatyzacji
CPV – 32420000-3 urządzenia sieciowe

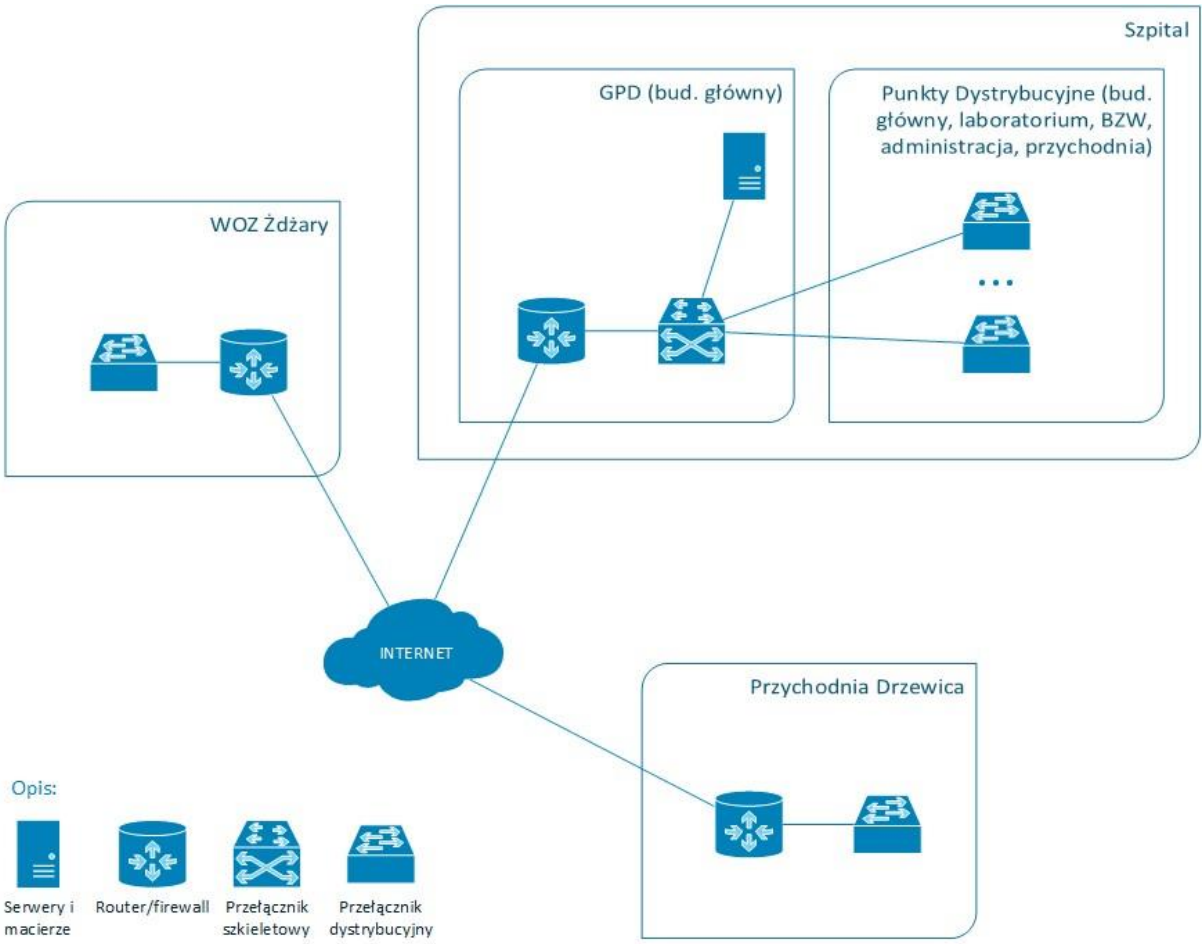
Spis treści

1. Wstęp

Przedmiotem niniejszego opracowania jest program funkcjonalno-użytkowy zaprojektowania i budowy oraz wymagania dla instalacji okablowania strukturalnego informatycznego wraz z dedykowaną instalacją elektryczną dla potrzeb zasilania Punktów Dystrybucyjnych w budynkach Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Nowym Mieście nad Pilicą, Przychodni Rejonowej w Drzewicy oraz w Ośrodku Zdrowia w Żdżarach .

W celu osiągnięcia wysokiej efektywności realizacji świadczeń medycznych konieczne jest zapewnienie infrastruktury niezbędnej do działania eUsług, tj. infrastruktury teletechnicznej, okablowania sieciowego (LAN), punktów dystrybucyjnych, centrum przetwarzania danych (serwerowni), sieciowych urządzeń aktywnych oraz zasilania. Wspomniana infrastruktura powinna tworzyć środowisko do działania eUsług, które będzie zapewniało ich wysoką dostępność, bezpieczeństwo i szybkość działania.

Poniższy schemat przedstawia planowaną strukturę logiczną środowiska informatycznego.



W związku z powyższym istniejąca w szpitalu infrastruktura musi ulec modernizacji i rozbudowie, aby umożliwić szybką, bezpieczną i bezawaryjną obsługę pacjenta w każdym punkcie udzielania świadczeń medycznych w szpitalu.

Zamawiający chcąc dokonać możliwie największego przybliżenia skali problemu oraz umożliwić proces należytego oszacowania kosztów wykonania planowanych przedsięwzięć w zakresie budowy sieci informatycznej w obiekcie SP ZOZ w Nowym Mieście zaprasza zainteresowanych na dokonanie wizji lokalnej na terenie objętym przedmiotem zamówienia. Wykonawcy mogą dokonywać wizji po uprzednim telefonicznym uzgodnieniu terminu z Zamawiającym.

2. Uproszczony opis prac

Należy zaprojektować i wykonać od podstaw sieć informatyczną Kategorii 6A/ Klasa EA oraz dedykowaną sieć elektryczną dla potrzeb Punktów Dystrybucyjnych w sześciu budynkach SP ZOZ Nowe Miasto nad Pilicą oraz w jednym budynku Przychodni w Drzewicy i jedynym budynku Ośrodka Zdrowia w Żdżarach.

Serwerownię zlokalizowaną w budynku Izby Przyjęć wyposażyć w szafę informatyczną wraz z niezbędnymi urządzeniami takimi jak: serwery, macierz, przełączniki sieciowe, zasilaczy UPS.

W drugiej Serwerowni zlokalizowanej w budynku ADM dostarczyć szafę informatyczną wraz z niezbędnymi urządzeniami takimi jak: serwer backupowy, biblioteka taśmowa, przełączniki sieciowe, zasilaczy UPS.

Ponadto w Serwerowniach należy dostarczyć i zainstalować klimatyzację oraz system kontroli dostępu, SSWiN, system monitoringu środowiska z czujką dymu, temperatury i zalania wody.

Punkty Dystrybucyjne wyposażyć w sieciowe elementy pasywne i aktywne niezbędne do prawidłowego funkcjonowania sieci wraz z zasilaczem UPS do podtrzymania zasilania.

3. Minimalne wymagania, opis wykonania i standardy dotyczące sytemu i komponentów okablowania strukturalnego

3.1 Sieć logiczna

Wykonawca jest zobligowany w ramach przedstawionej przez siebie oferty zaproponować realizację przedmiotu zamówienia, stanowiącego łącznie sieć informatyczną w jednorodnym rozwiązaniu systemu okablowania strukturalnego. Wszystkie elementy pasywne okablowania strukturalnego (światłowodowego i miedzianego) muszą pochodzić z jednolitej oferty reprezentującej kompletny system w takim zakresie, żeby możliwe było uzyskanie certyfikatu gwarancyjnego potwierdzającego co najmniej 25-letni okres gwarancji systemowej.
System okablowania musi bezwzględnie spełniać wszystkie podane wymagania:

a) Okablowanie poziome w formie uniwersalnego okablowania strukturalnego w wersji ekranowanej, klasa EA, (okablowanie F/FTP kat. 6A LSOH) gwarantujące przepustowość binarną na poziomie 10Gbps. Okablowanie szkieletowe światłowodowe, multimodowe klasy OM4.

b) Wszystkie komponenty systemu okablowania mają być zgodne wymaganiami obowiązujących norm:

- PN-EN 50173-1:2011 Technika informatyczna – Systemy okablowania strukturalnego – Część 1: Wymagania ogólne.
- PN-EN 50173-2:2008/A1:2011 Technika informatyczna – Systemy okablowania strukturalnego – Część 2: Pomieszczenia biurowe.
- PN-EN 50174-2:2010/A2-2015-02 Technika informatyczna – Instalacja okablowania – Część 2: Planowanie i wykonywanie instalacji wewnątrz budynków.
- PN-EN 50174-1:2010/A2-2015-02 Technika informatyczna – Instalacja okablowania – Część 1: Specyfikacja instalacji i zapewnienia jakości.
- PN-EN 50346:2004/A2:2010 Technika informatyczna – Instalacja okablowania – Badanie zainstalowanego okablowania.
- Inernational standard ISO/IEC 11801: Information technology – Generic cabling for customer premises.

c) Producent okablowania musi spełniać normy standardów jakości ISO 9001 oraz spełniać normy zarządzania środowiskiem zgodnie z normą ISO 14001. Całość instalacji okablowania strukturalnego miedzianego powinna być przetestowana na zgodność z klasą EA przy zastosowaniu miernika z pomiarem dynamicznym o poziomie dokładności pomiaru co najmniej level IV.

d) System okablowania strukturalnego musi posiadać certyfikaty wydane przez niezależne laboratorium badawcze, np. GHMT. Delta, 3P, które potwierdzają wydajność klasy EA.

e) Minimalne wymagania elementów pasywnych miedzianego toru transmisyjnego okablowania strukturalnego

- **Kabel instalacyjny F/FTP kat.6A**

  Kabel typu skrętka podwójnie ekranowany F/FTP (PiMF) kat.6A 500MHz LSOH

  - zgodność z normami:
    - kategoria 6A zgodnie z: EN 50288-10 do 500MHz, IEC 61156-5,
    - odporność na spalanie: IEC 60332-1, EN 50266-2-1,
    - wydzielanie gazów podczas spalania: IEC 60754-2, EN 50267,
    - wydzielanie dymów podczas spalania: IEC 61034, EN 50268,
  - przeznaczony do instalacji pionowych i poziomych w strukturalnym okablowaniu budynku,
  - przewód: drut miedziany, AWG 23,
  - ekran:
    - każda para indywidualnie ekranowana folią metalową (PiMF),
    - wszystkie pary łącznie ekranowane folią metalową,
  - budowa przewodu: 4 zwinięte pary indywidualnie ekranowane,
  - płaszcz ochronny: LSZH (Low Smoke Zero Halogen),
  - średnica zewnętrzna: ≤7,5mm,
  - nominalna prędkość propagacji (NVP): 0,79c,
  - waga kabla: ≤50kg/km;
  - obciążalność ogniowa: min. 550kJ/m,
  - zakres temperatur-eksploatacja/składowanie: -20oC do +60oC,
  - zakres temperatur-instalacja: 0oC do +50oC,
  - min. promień gięcia-eksploatacja: 22mmm,
  - min. promień gięcia-instalacja: 55mm,
  - max. siła ciągnięcia: max. 145N.

- **Moduł RJ45 keystone kat.6A ekranowany**

  - kategoria potwierdzona certyfikatem niezależnego laboratorium na zgodność z normami:

    ISO/IEC 11801 AMD 2 (2010-04),

    IEC 60603-7-51 Ed. 1 (IEC 48B/1977/CDV, 2008/12),
  - możliwość ponownego zarobienia na kablu instalacyjnym bez konieczności jego wymiany,
  - moduły z klapką antykurzową występującą w przynajmniej czterech kolorach w celu zapewnienia identyfikacji poszczególnych portów w panelu krosowym,
  - konstrukcja z pełnym ekranowaniem 360^{o},
  - zarabiany beznarzędziowo,
  - te same moduły montowane w panelu krosowym i w gnieździe abonenckim
  - możliwość rozszycia wg schematu T568A i T568B.

- **Panel krosowy 24 porty, modularny, niewyposażony**
  - możliwość montażu modułów RJ45 typu keystone,
  - kabel PE,
  - zawiera zestaw montażowy (nakrętka klatkowa, śruby i podkładki M6),
  - masywny uchwyt kablowy.

- **Kable krosowe S/FTP kat.6A RJ45**
  - długości od stronu punktu PEL od 2m do 5m (zależna od rozmieszczenia stanowisk komputerowych),
  - długości do połączeń aktywnych i pasywnych elementów sieci w szafach dystrybucyjnych od 0,5m do 2 m,

f) Minimalne wymagania elementów pasywnych światłowodowego toru transmisyjnego okablowania strukturalnego

- **Kabel światłowodowy multimodowy 12-włóknowy OM4**
  - budowa: centralna tuba wypełniona żelem (niewypływającym i niezawierającym silikonu),
  - wzmocnione szkliwem włókna aramidowe zabezpieczające przez wodą oraz chroniące przed gryzoniami,
  - promień gięcia:
    ≥15 x średnica zewn. podczas eksploatacji,
    ≥10 x średnica zewn. podczas instalacji
  - spełniający normy:
    IEC 60794-1-2-F5 (wzdłużna wodoszczelność),
    IEC 60332-3C / EN 50266-2-4 (ognioodporność),
    IEC 61034 (wydzielanie gazów podczas spalania).

- **Panel krosowy światłowodowy**
  - wysokość 1U, szer. 19”,
  - kompletny z wysuwaną szufladą, wyposażony w odpowiednią ilość kaset na spawy, pigtaile, oraz adaptery LC duplex MM OM4,
  - adaptery wyposażone w samozamykające się klapki przeciw kurzowe z metalową sprężynką, będące integralną częścią adaptera (każdy adapter wyposażony w piktogram informujący o możliwym zagrożeniu promieniowaniem optycznym),
  - niewyposażone porty wypełnione fabrycznymi zaślepkami,
  - wejścia kablowe za złączami dławikowymi.

- **Kable krosowe światłowodowe**

- kable MM OM4 duplex LC-LC,
- długość stosowane w Punktach Dystrybucyjnych: 1m,
- długość stosowane w Głównym Punkcie Dystrybucyjnym: 2m.

g) Minimalne wymagania dla szafy 24U 600mm x 800mm

Szafa zostanie dostarczona z następującym wyposażeniem (lub równoważne) – 2 komplety:

- Szafa teleinformatyczna o wymiarach:
  szerokość: 600 mm, głębokość: 800 mm, wysokość: 24U),
- rodzaj drzwi i osłon bocznych:
  - drzwi przednie drzwi szklane, szkło hartowane,
  - drzwi tylne drzwi blaszane pełne,
  - lewy bok osłona blaszana pełna,
  - prawy bok osłona blaszana pełna,
- rodzaj dachu: dach z otworami pod zaślepki,F
- dwie pary belek nośnych 19",
- listwa zasilająca 9 gniazdowa,
- panel wentylacyjny dachowy czterowentylatorowy.

h) Minimalne wymagania dla szafy wiszącej 12U 600mm x 800mm

Szafa zostanie dostarczona z następującym wyposażeniem (lub równoważne) – 2 komplety:

- Szafa teleinformatyczna, wisząca, dwusekcyjna o wymiarach:
  szerokość: 600 mm, głębokość: 500 mm, wysokość: 12U),
- rodzaj drzwi i osłon bocznych:
  - drzwi przednie drzwi szklane, szkło hartowane,
  - lewy bok osłona blaszana pełna,
  - prawy bok osłona blaszana pełna,
- rodzaj dachu: dach z otworem perforowanym dla wentylatora,
- jedna para belek nośnych 19",
- listwa zasilająca 9 gniazdowa.

i) W fazie projektowej należy skonfigurować gniazda końcowe według wytycznych użytkownika, tak aby spełniały obecne jego wymagania użytkowe, każdy punkt przyłączeniowy PEL okablowania strukturalnego będzie składał się z dwóch linii Kat.6A RJ45 (PEL=2xRJ45),

j) Instalacja okablowania systemu sieci LAN powinna zawierać w ramach realizacji usługę instalacji kompletnego toru kablowego z koniecznymi do wykonania pracami instalacyjnymi (wykonanie kanalizacji teletechnicznej, przepustów w stropach lub ścianach działowych dla okablowania).

k) Instalację szkieletowego okablowania światłowodowego należy zaprojektować i wykonać:

- pomiędzy budynkami w kanalizacji teletechnicznej,

- wewnątrz poszczególnych budynków w listwach PCV oraz korytach metalowych.

l) Instalacja poziomego okablowania logicznego należy zaprojektować i wykonać w listwach PCV oraz korytach metalowych. Ponadto moduły zainstalowane muszą zostać ponumerowane w sposób trwały i widoczny.

m) Punkty PEL powinny występować w formie gniazd natynkowych, umiejscowionymi nad lub pod torami kablowymi.

n) Istniejąca kanalizacja teletechniczna Zamawiającego nie jest doprowadzona do wszystkich budynków objętych planem budowy sieci teleinformatycznej. Należy zaprojektować
i wykonać brakujące odcinki kanalizacji teletechnicznej umożliwiając połączenie wszystkich planowanych punktów dystrybucyjnych okablowaniem światłowodowym z Głównym Punktem Dystrybucyjnym.

o) Zamawiający nie dopuszcza realizacji połączeń stanowisk lub poszczególnych segmentów sieci budynkowej z wykorzystaniem połączeń bezprzewodowych. Planowana sieć bezprzewodowa ma służyć podłączeniu tabletów używanych przez lekarzy
z projektowanym systemem medycznym.

p) Wykonawca zapewni w ramach wykonania usługi odpowiednią ilość przewodów krosowych (z zachowaniem kat.6A) dla realizacji połączeń jednostek komputerowych z pobudowanym torem logicznym (długość zależna od rozmieszczenia stanowisk komputerowych od 2m do 5m) oraz niezbędnych do połączeń aktywnych i pasywnych elementów sieci w szafach dystrybucyjnych (od 0,5m do 2 m).

q) Kable transmisyjne – zgodnie z normą – muszą być zakończone w sposób trwały na 8-pozycyjnym złączu; nie są dopuszczalne zmiany i rekonfiguracje rozszycia w trakcie pracy systemu. Złącza kablowe mają być zakańczane za pomocą standardowych narzędzi instalacyjnych, tj. narzędzia uderzeniowego typu 110 lub narzędzia LSA+. Zalecane są takie sposoby terminacji kabla, które pozwalają zakończyć w jednym ruchu narzędzia wszystkie pary transmisyjne z minimalnym rozplotem.

r) Zastosowane materiały muszą posiadać atesty dopuszczające do stosowania w budownictwie.

s) Zamawiający informuje, że wskazane w specyfikacji typy i symbole materiałów lub urządzeń oraz nazwy ich producentów zostały określone w celu sprecyzowania parametrów i warunków techniczno-użytkowych przedmiotu zamówienia. Zamawiający dopuszcza oferowanie materiałów i urządzeń równoważnych, pod warunkiem, że zagwarantują one uzyskanie parametrów technicznych i eksploatacyjnych nie gorszych od założonych w dokumentacji. W przypadku zastosowania innych niż podane rozwiązań, udowodnienie równoważności proponowanych rozwiązań spoczywa na Wykonawcy. Nie wykazanie materiałów równoważnych traktowane będzie, jako deklaracja wbudowania materiałów wymienionych w dokumentacji przetargowej.

3.2 Sieć elektryczna

a) Instalacja okablowania systemu zasilania dedykowanego dla budowanego systemu sieci LAN ma obejmować zasilanie Serwerowni, Głównego Punktu Dystrybucyjnego oraz wszystkie Punkty Dystrybucyjne. Powinna zawierać w ramach realizacji usługę instalacji kompletnego toru energetycznego z koniecznymi do wykonania pracami instalacyjnymi (wykonanie przepustów w stropach lub ścianach działowych dla okablowania, instalację dedykowanej tablicy rozdzielczej dla serwerowni wraz z kompletem wymaganych przepisami SEP przełączników automatyki w zabezpieczeniu obwodów).

b) Dla zasilania Serwerowni Podstawowej należy zaprojektować dedykowaną rozdzielnię elektryczną zasilaną z rozdzielni głównej Budynku Izby Przyjęć. Należy zaprojektować minimum trzy dedykowane obwody dla zasilania urządzeń w szafie serwerowej. Jeden dedykowany obwód zasilający do zasilania urządzeń SSWiN i KD oraz dedykowane obwody do zasilania urządzeń klimatyzacji.

c) Dla zasilania Drugiej Serwerowni oraz Głównego Punktu Dystrybucyjnego należy zaprojektować dwa dedykowane obwody. Dedykowane obwody należy zasilić z lokalnej rozdzielni elektrycznej. Każdy obwód elektryczny musi zostać zabezpieczony wyłącznikiem różnicowoprądowym i nadprądowym.

d) Należy zaprojektować dedykowany obwód dla zasilania urządzeń każdego Punktu Dystrybucyjnego. Dedykowane obwody zasilające Punkty Dystrybucyjne należy zasilić z lokalnych rozdzielni elektrycznych. Każdy obwód elektryczny musi zostać zabezpieczony wyłącznikiem różnicowoprądowym i nadprądowym.

e) Dedykowana sieć zasilająca musi mieć prawidłowo zabezpieczoną wartość poziomu uziomu, zgodnie z przepisami szczegółowymi dla tego typu działania oraz przepisami wykonawczymi SEP i norm Prawa Budowlanego.

f) Do budowy toru zasilającego koniecznym jest użycie przewodów izolowanych YDY – 750 V 3x2,5 mm^2 lub innych o porównywalnych parametrach izolacyjno-eksploatacyjnych.

g) Każdą szafę serwerową/dystrybucyjną należy uziemić przewodem izolowanym LGY 10$mm.^2$

h) Po zakończeniu prac instalacyjnych należy wykonać pomiary sprawdzające zgodnie z normą PN-HD 60364-6/2008.

i) System zasilania powinien zostać poprowadzony w listwach natynkowych PCV lub korytach metalowych.

j) Wszystkie korytka metalowe, drabinki kablowe, szafy kablowe i serwerowe wraz z osprzętem oraz urządzenia aktywne sieci teleinformatycznej muszą być uziemione by zapobiec powstawaniu zakłóceń.

3.3 Sposób wykonania

a) Wykonawca wykona i przedłoży do weryfikacji Zamawiającemu dokumentację projektową zgodnie z obowiązującym Rozporządzeniem Ministra Infrastruktury w sprawie szczegółowego zakresu i formy dokumentacji projektowej, specyfikacji

technicznych wykonania i odbioru robót budowlanych oraz programu funkcjonalno-użytkowego z dnia 2 września 2004 r. (Dz. U. Nr. 202, poz. 2072).

b) Zamawiający nie dopuszcza montażu torów kablowych na żadnym z odcinków na kleje natynkowe, a jedynie z wykorzystaniem kołków montażowych.

c) Zamawiający nie dopuszcza przeciągania przewodów toru kablowego przez przepusty ścianowe i między stropowe – bez wprowadzania w nie peszli lub rur sztywnych PCV.

d) Wykonawca zaprojektuje trasy torów kablowych w zakresie całego projektu po szczegółowych uzgodnieniach z Zamawiającym.

e) Wykonawca prowadząc tory kablowe dla sieci strukturalnej jest zobligowany do szczególnej ostrożności w czasie realizacji odwiertów przez ściany działowe lub między stropowe
w zakresie istniejących wiązek elektryki ogólnej, linii telefonicznej, której położenie na obiekcie nie jest udokumentowane schematem instalacyjnym.

f) Wszelkie uszkodzenia infrastruktury ogólnej na obiekcie przez Wykonawcę podczas prowadzenia prac instalacyjnych obciążają jego samego i muszą być usunięte w ramach nieodpłatnego usunięcia szkód w terminie natychmiastowym po ich stwierdzeniu.

g) Zamawiający wymaga, aby Wykonawca we własnym zakresie zapewnił składowanie i sprzątanie odpadów.

h) Wykonawca zobowiązany jest do pozostawienia pomieszczeń w których będą wykonywane prace w stanie takim jaki zastał przed przystąpieniem do prac.

i) Wszelkie wykończenia okablowania, w tym szycie na krosownicach szafy dystrybucyjnej oraz poszczególnych punktów dostępowych Wykonawca powinien wykonać z zachowaniem norm dla standardu Ethernet w kat. 6A. Dokładne wytyczne dotyczące uprawnień oraz certyfikatów instalatorów okablowania zawarte zostały w punkcie 6 opracowania.

j) Zamawiający zaleca dokonać wizję lokalną obiektu celem samodzielnej weryfikacji prac koniecznych do wykonania, tj. przeloty, odwierty w ścianach działowych, rozpoznanie istniejących tablic energetycznych itp. – dla prawidłowego oszacowania czasu realizacji wykonania przedmiotu zamówienia oraz jego wyceny. Zaleca się także dokonania subiektywnego określenia na potrzeby wykonania wyceny i projektu oszacowania poziomu trudności prac i ilości koniecznych do zastosowania materiałów oraz weryfikacje przygotowanych przez Zamawiającego długości torów kablowych.

k) Wykonawca zobowiązany jest prowadzić prace objęte przedmiotem zamówienia

l) Wykonawca przed przystąpieniem do projektowania budowy sieci zobowiązany jest do doprecyzowania dokładnego rozmieszczenia punktów PEL w poszczególnych pomieszczeniach.

m) Wykonawca po ukończonej realizacji okablowania – dokona pomiaru punktów zasilania w zakresie prawidłowego zadziałania systemów przepięciowych i różnicowoprądowych – zgodnie z obowiązującymi normami, co zostanie ujęte protokołem pomiarowym na moment zgłoszenia przez Wykonawcę sieci do odbioru Zamawiającemu.

n) Sieć logiczna oraz zasilanie dedykowane dla sieci LAN będzie podlegało odbiorowi końcowemu – przez Wykonawcę poprzez przeprowadzenie testów akceptacyjnych dla punktów dostępowych na obiekcie.

o) Wykonawca po zakończonych pracach instalacyjnych – dokona pomiarów poszczególnych segmentów z wykorzystaniem miernika pomiarowego, posiadającego aktualną kalibracje potwierdzoną przez producenta miernika. Szczegółowy wykaz pomiarów jakie należy wykonać został zawarty w punkcie 8 opracowania.

p) Wykonawca jest zobowiązany do wykonania dokumentacji powykonawczej w postaci papierowej oraz elektronicznej na nośniku CD/DVD w formacie pdf, gdzie schematy sieci elektrycznej oraz logicznej zapisane będą zawierały informacje o rozmieszczeniu gniazd i ułożeniu kabli zasilających, prowadzenie torów kablowych na obiekcie, schemat połączeń fizycznych z opisem obwodów oraz oznaczeniem tablic. Wykonawca nie jest zobowiązany do przeprowadzenia inwentaryzacji istniejących struktur sieci energetycznych, telefonicznych oraz umiejscowienia ich w swojej dokumentacji, realizowanej w zakresie niniejszego projektu.

q) Dokumentacja Techniczna powinna być zaopatrzona w pisemne oświadczenie projektanta. Iż jest wykonana zgodnie z umową, obowiązującymi przepisami oraz normami i że została wydana w stanie kompletnym z punktu widzenia celu któremu ma służyć. Niniejsze oświadczenie stanowić będzie integralną część dokumentacji.

4. Szczegóły dotyczące budowy sieci informatycznej

4.1 Założenie ogólne

Celem niniejszego projektu jest wykonanie od podstaw nowej sieci w Kategorii 6A/Klasa EA w budynkach:

- Szpital,
- Laboratorium,
- Przychodnia Rejonowa,
- Budynek Administracji,
- Portiernia,
- Stacja karetek Pogotowia Ratunkowego,
- Budynek Przychodni Rejonowej w Drzewicy przy ul. Stawowej 27.
- Budynek Ośrodka Zdrowia w Żdżarach 75C .

a) Kanalizacja teletechniczna dla połączenia okablowaniem światłowodowym poszczególnych punktów dystrybucyjnych rozmieszczonych w budynkach z Głównym Punktem Dystrybucyjnym przy ul. Tomaszewskiej 43.

b) Minimalne wymagania elementów okablowania komputerowego według wymagań opisanych powyżej w punkcie 3.

c) Ilość stanowisk roboczych wynika z ustaleń z Zamawiającym, przy czym ich ostateczna i precyzyjna lokalizacja powinna być ustalona z Zamawiającym podczas projektowania instalacji.

Zestawienie ilościowe PEL w poszczególnych punktach dystrybucyjnych budynków Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Nowym Mieście nad Pilicą przy ulicy Tomaszewskiej 43.

Punkt dystrybucyjny	Lokalizacja punktu dystrybucyjnego	Planowana ilość PEL (2xRJ45)	Planowana ilość AP (1xRJ45)	Rodzaj szafy	Połączenia światłowodowe
SVR	Izba Przyjęć	-	-	stojąca 42U	MM 12x50/125 OM4 - GPD
PD1	Szpital	66	10	stojąca 42U	MM 12x50/125 OM4 - GPD
PD2	Laboratorium	32	0	stojąca 24U	MM 12x50/125 OM4 - GPD
PD3	Przychodnia Rejonowa	41	0	stojąca 24U	MM 12x50/125 OM4 - GPD
GPD, PD4	Budynek Administracji	30	0	stojąca 42U	MM 12x50/125 OM4 – SVR MM 12x50/125 OM4 – PD1 MM 12x50/125 OM4 – PD2 MM 12x50/125 OM4 – PD3 MM 12x50/125 OM4 – PD5 MM 12x50/125 OM4 – PD6
PD5	Stacja Karetek	5	0	wisząca	MM 12x50/125 OM4 - GPD

	Pogotowia Ratunkowego			12U	
PD6	Portiernia	5	0	wisząca 12U	MM 12x50/125 OM4 - GPD
PD7	Izba Przyjęć	-	-	Istniejąca stojąca 42U 600x600	MM 12x50/125 OM4 - GPD

Dodatkowo dla potrzeb sieci bezprzewodowych (sieć WiFi) na terenie Szpitala powstanie 10 punktów logicznych do podłączenia planowanych punktów dostępowych z wykorzystaniem technologii PoE.

Zestawienie ilościowe PEL w punkcie dystrybucyjnym budynku Przychodni Rejonowej Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Nowym Mieście nad Pilicą w miejscowości Drzewica przy ulicy Stawowej 27.

Punkt dystrybucyjny	Lokalizacja punktu dystrybucyjnego	Planowana ilość PEL	Rodzaj szafy	Połączenia światłowodowe
BPD	Drzewica ul. Stawowa 27	26	stojąca 24U	-

Zestawienie ilościowe PEL w punkcie dystrybucyjnym budynku Ośrodka Zdrowia Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Nowym Mieście nad Pilicą w miejscowości Żdżary 75C.

Punkt dystrybucyjny	Lokalizacja punktu dystrybucyjnego	Planowana ilość PEL	Rodzaj szafy	Połączenia światłowodowe
BPD	Żdżary 75C	10	Stojąca/wisząca 24U	-

4.2 Trasy kablowe

4.2.1 Kanalizacja teletechniczna dla połączenia okablowaniem światłowodowym poszczególnych punkty dystrybucyjnych z Głównym Punktem Dystrybucyjnym

Istniejąca kanalizacja teletechniczna Zamawiającego nie jest doprowadzona do wszystkich budynków przy ul. Tomaszowskiej 43 objętych planem budowy sieci teleinformatycznej, ponadto kanalizacja może być odcinkami niedrożna. Należy zaprojektować i wykonać brakujące odcinki kanalizacji teletechnicznej umożliwiając połączenie wszystkich planowanych punktów dystrybucyjnych okablowaniem światłowodowym z Głównym Punktem Dystrybucyjnym. Zamawiający zaleca wizję lokalną w celu prawidłowej wyceny przez Oferentów praz związanych z kanalizacja teletechniczną.

Należy zaprojektować i wykonać kanalizację kablowa pierwotną z rur DVR 110 oraz rur RHDPE 110/6,3 pod drogami i kanalizację wtórną RHDPE 32/2. Pomiędzy przęsłami kanalizacji kablowej należy wybudować studnie SKR1 z pokrywami typu ciężkiego. Rury należy układać na głębokości min. 0,7m od powierzchni terenu, a pod drogami na głębokości min. 1m od nawierzchni dróg. Podaną głębokość ułożenia liczyć do górnej powierzchni kanalizacji. Rury łączyć złączkami szczelnymi. Nad rurociągiem w połowie wykopu ułożyć taśmę ostrzegawczą z napisem "UWAGA! KABEL TELEKOMUNIKACYJNY". Rury układać na podsypce piaskowej grubości 5cm, przykrywając od góry warstwą piasku grubości 10cm. Wykop należy zasypać po ułożeniu całego ciągu rur warstwami grubości do 20cm, używając ziemi z urobku i ubijać mechanicznie. Wejścia kanalizacji do budynków oraz wejścia rurociągów do studni SKR należy odpowiednio uszczelnić.

W związku z istniejącym uzbrojeniem podziemnym Zamawiający przewiduje konieczność wykonana wszelkich prac przy budowie kanalizacji kablowej metodą ręczną, zaś przejścia pod drogami należy wykonać metodą ‘przecisku’ lub ‘odwiertu kierowanego’.
Kanalizację kablową należy budować przy zachowaniu normatywnych odległości od innych urządzeń uzbrojenia nad i podziemnego, zgodnie z obowiązującymi wymaganiami norm branżowych oraz rozporządzeniami właściwych ministrów.

4.2.2 Trasy kablowe wewnątrz budynków

Okablowanie strukturalne wewnątrz budynków ma być prowadzone w korytach metalowych oraz kanałach PCV. Wykonane kanały kablowe powinny umożliwiać zapas pojemności minimum 30%. Przebieg tras kablowych należy uzgodnić na etapie projektu z Zamawiającym.

Należy stosować następujące rozmiary koryt:

- koryta metalowe:
  - 300x60 grubość blachy min. 0,7mm,
  - 200x60 grubość blachy min. 0,7mm,
  - 100x60 grubość blachy min. 0,7mm,
  - 60x60 grubość blachy min. 0,7mm,

Gwarancją jakości materiału PCV użytego do wykonania systemu jest znak CE w oparciu o normę PN-EN 50085-1:2001 Systemy listew instalacyjnych otwieranych i listew instalacyjnych zamkniętych do instalacji elektrycznych - Cześć 1: Wymagania ogólne. Przy projektowaniu tras kablowych należy zachować wymagane odległości od innych instalacji zgodnie z obowiązującymi normami.

Przed przystąpieniem do montażu koryt kablowych należy sprawdzić instalacje już istniejące w ścianach i w zależności od ich położenia odpowiednio dobrać trasy montażu kanałów.

4.3 Okablowanie strukturalne

Punkt końcowy PEL oparty jest na gnieździe informatycznym z dwoma wejściami RJ45, celem jak największej uniwersalności i możliwości adaptacji do dowolnego systemu osprzętu teleinformatycznego.

4.3.1 Szkieletowe okablowanie światłowodowe

Szkieletowe okablowanie światłowodowe ma zapewnić przepustowość 10 Gb/s pomiędzy poszczególnymi punktami dystrybucyjnymi a głównym punktem dystrybucyjnym. Powinno zostać wykonane kablami światłowodowymi multimodowymi 12-włóknowymi OM4 zgodnie z wymaganiami w punkcie 3. Podczas układania kabla światłowodowego należy przewidzieć zapas kabla na zarobienie złącz (ok. 2 mb. z każdej strony kabla, nadmiar włókien zwinąć w panelach światłowodowych) oraz zapas technologiczny 5 mb. po obu stronach zwinięty w szafach oraz 5 mb. w każdej studni kanalizacji teletechnicznej.

4.3.2 Okablowanie poziome

Okablowanie strukturalne obejmuje łącznie 205 gniazd logicznych podwójnych PEL (PEL=2xRJ45). Szczegółowe rozmieszczenie i lokalizację punktów PEL należy ustalić z Zamawiającym. Okablowanie poziome zostanie rozprowadzone w torach kablowych (koryta metalowe oraz PCV) zgodnie z wytycznymi z poprzednich punktów opracowania, nad lub pod którymi należy zamontować puszki z gniazdami logicznymi. Prowadzenie tras kablowych, kanałów musi zostać ustalone z Zamawiającym podczas projektowania instalacji. Należy stosować kable w powłokach trudnopalnych LSZH. Kabel ten ma spełniać wymagania stawiane komponentom opisanym w punkcie 3**,** równocześnie zapewniając pełną zgodność z niższymi kategoriami okablowania. Kable instalacyjne należy zakończyć w szafach kablowych w punktach dystrybucyjnych panelach 24 – portowych. Od strony paneli krosowych w szafach dystrybucyjnych należy zostawić zapas kabla skrętkowego ok. 3 m. Od strony punktu abonenckiego [PEL] należy zostawić zapas kabla skrętkowego na ewentualne ponowne rozszycie kabla na module RJ45. Przy rozszyciu kabla należy zastosować sekwencję 568B.

4.3.3 Punkty dystrybucyjne

4.3.3.1 SVR - Serwerownia Podstawowa

W nowo wybudowanym budynku Izby Przyjęć w piwnicy budynku w pomieszczeniu nr 1.09 zaplanowano Podstawowa Serwerownię, w której przewidziano szafę 42U 800x1000 na sprzęt serwerowy, opis szafy punkt 12.8. Szafa serwerowa z wyposażeniem.

Do połączenia powyższej szafy z Głównym Punktem Dystrybucyjnym przewidziano szkieletowe połączenie światłowodowe kablem wielomodowym 12-włóknowym 50/125µm OM4 FRNC/LSOH-3. Kabel światłowodowy należy zakończyć w przełącznicy światłowodowej 12xLC (6xLC duplex) metodą spawania.

Szafę 42U 800mm x 1000mm należy wyposażyć w:

- 1x przełącznica światłowodowa 1U 12xLC (6xLC duplex) OM4,
- 2x organizator kablowy 1U z wieszakami.

Zasilanie szafy

Dla zasilania Serwerowni Podstawowej zaplanowano dedykowaną rozdzielnię elektryczną zasilaną z rozdzielni głównej Budynku Izby Przyjęć. Zaplanowano dwa dedykowane obwody dla zasilania urządzeń w szafie serwerowej. Szafę należy uziemić

4.3.3.2 GPD – Główny Punkt Dystrybucyjny / Druga serwerownia

W budynku Administracji na pierwszym piętrze w pomieszczeniu nr 114 zaplanowano drugą serwerownię, w której przewidziano szafę 42U 800x1000 na sprzęt serwerowy oraz Główny Punkt Dystrybucyjny [GPD] i Punkt Dystrybucyjny [PD4] dla budynku Administracji, opis szafy punkt 12.8. Szafa serwerowa z wyposażeniem.

W powyższej szafie schodzić będzie się szkieletowe okablowanie światłowodowe z pozostałych Punktów Dystrybucyjnych oraz Podstawowej Serwerowni [PD1, PD2, PD3, PD5, PD6, PD7, SVR], łącznie 7 połączeń światłowodowych wykonanych kablem wielomodowym 12-włóknowym 50/125µm OM4 FRNC/LSOH-3. Kable światłowodowe należy zakończyć w przełącznicach światłowodowych 24xLC (12xLC duplex) metodą spawania.

W powyższej szafie schodzić będzie się poziome okablowanie miedziane z budynku Administracji, łącznie 60 linii LAN wykonanych kablem F/FTP kat.6A 500MHz LSOH. Kable miedziane należy zakończyć na panelach krosowych 1U 24-portowych.

Szafę 42U 800mm x 1000mm należy wyposażyć w:

- 4x przełącznica światłowodowa 1U 24xLC (12xLC duplex) OM4,
- 3x panel krosowy 24-portowy niewyposażony,
- 60x moduł keystone RJ45 kat.6A ekranowany,
- 7x organizator kablowy 1U z wieszakami.

Zasilanie szafy

Dla zasilania Drugiej Serwerowni oraz Głównego Punktu Dystrybucyjnego zaplanowano dwa dedykowane obwody zasilające. Dedykowane obwody należy zasilić z

lokalnej rozdzielni elektrycznej. Każdy obwód elektryczny musi zostać zabezpieczony wyłącznikiem różnicowoprądowym i nadprądowym. Szafę należy uziemić.

4.3.3.3 PD1 – Punkt Dystrybucyjny – budynek Szpitala

Punkt Dystrybucyjny okablowania strukturalnego dla budynku Szpitala zaplanowano w pomieszczeniu nr 22 na parterze, w którym przewidziano szafę 42U 800x1000, opis szafy punkt 12.8. Szafa serwerowa z wyposażeniem.

W PD1 schodzić będzie się poziome okablowanie miedziane z budynku Szpitala, łącznie 142 linie LAN wykonanych kablem F/FTP kat.6A 500MHz LSOH. Kable miedziane należy zakończyć na panelach krosowych 1U 24-portowych

Do połączenia PD1 z Głównym Punktem Dystrybucyjnym przewidziano szkieletowe połączenie światłowodowe kablem wielomodowym 12-włóknowym 50/125µm OM4 FRNC/LSOH-3. Kabel światłowodowy należy zakończyć w przełącznicy światłowodowej 12xLC (6xLC duplex) metodą spawania.

Szafę 42U 800mm x 1000mm należy wyposażyć w:

- 1x przełącznica światłowodowa 1U 24xLC (12xLC duplex) OM4,
- 6x panel krosowy 24-portowy niewyposażony,
- 142x moduł keystone RJ45 kat.6A ekranowany,
- 13x organizator kablowy 1U z wieszakami.

Zasilanie szafy

Dla zasilania szafy PD1 dedykowany obwód zasilający z lokalnej rozdzielni elektrycznej. Dedykowany obwód elektryczny musi zostać zabezpieczony wyłącznikiem różnicowoprądowym i nadprądowym. Szafę należy uziemić.

4.3.3.4 PD2 – Punkt Dystrybucyjny – Laboratorium

Punkt Dystrybucyjny okablowania strukturalnego dla budynku Laboratorium zaplanowano w pomieszczeniu nr 1 na parterze, w którym przewidziano szafę stojącą 24U, opis szafy punkt 12.8. Szafa serwerowa z wyposażeniem.

W PD2 schodzić będzie się poziome okablowanie miedziane z budynku Laboratorium, łącznie 64 linie LAN wykonanych kablem F/FTP kat.6A 500MHz LSOH. Kable miedziane należy zakończyć na panelach krosowych 1U 24-portowych

Do połączenia PD2 z Głównym Punktem Dystrybucyjnym przewidziano szkieletowe połączenie światłowodowe kablem wielomodowym 12-włóknowym 50/125µm OM4 FRNC/LSOH-3. Kabel światłowodowy należy zakończyć w przełącznicy światłowodowej 12xLC (6xLC duplex) metodą spawania.

Szafę 24U należy wyposażyć w:

- 1x przełącznica światłowodowa 1U 24xLC (12xLC duplex) OM4,
- 3x panel krosowy 24-portowy niewyposażony,
- 64x moduł keystone RJ45 kat.6A ekranowany,
- 7x organizator kablowy 1U z wieszakami.

Zasilanie szafy

Dla zasilania szafy PD2 dedykowany obwód zasilający z lokalnej rozdzielni elektrycznej. Dedykowany obwód elektryczny musi zostać zabezpieczony wyłącznikiem różnicowoprądowym i nadprądowym. Szafę należy uziemić.

4.3.3.5 PD3 – Punkt Dystrybucyjny – Przychodnia Rejonowa

Punkt Dystrybucyjny okablowania strukturalnego dla budynku Przychodni Rejonowej zaplanowano w piwnicy w pomieszczeniu po lewej stronie schodów, w którym przewidziano szafę stojącą 24U, opis szafy punkt 12.8. Szafa serwerowa z wyposażeniem.

W PD3 schodzić będzie się poziome okablowanie miedziane z budynku Przychodni Rejonowej, łącznie 82 linie LAN wykonanych kablem F/FTP kat.6A 500MHz LSOH. Kable miedziane należy zakończyć na panelach krosowych 1U 24-portowych

Do połączenia PD3 z Głównym Punktem Dystrybucyjnym przewidziano szkieletowe połączenie światłowodowe kablem wielomodowym 12-włóknowym 50/125µm OM4 FRNC/LSOH-3. Kabel światłowodowy należy zakończyć w przełącznicy światłowodowej 12xLC (6xLC duplex) metodą spawania.

Szafę 24U należy wyposażyć w:

- 1x przełącznica światłowodowa 1U 24xLC (12xLC duplex) OM4,
- 4x panel krosowy 24-portowy niewyposażony,
- 82x moduł keystone RJ45 kat.6A ekranowany,
- 9x organizator kablowy 1U z wieszakami.

Zasilanie szafy

Dla zasilania szafy PD3 dedykowany obwód zasilający z lokalnej rozdzielni elektrycznej. Dedykowany obwód elektryczny musi zostać zabezpieczony wyłącznikiem różnicowoprądowym i nadprądowym. Szafę należy uziemić.

4.3.3.5 PD5 – Punkt Dystrybucyjny – Stacja karetek Pogotowia Ratunkowego

Punkt Dystrybucyjny okablowania strukturalnego dla budynku Stacji Karetek Pogotowia Ratunkowego będzie stanowić szafka wisząca 12U, opis szafy punkt 12.8. Szafa serwerowa z wyposażeniem. Lokalizację należy zaplanować w uzgodnieniu z Zamawiającym.

W PD5 schodzić będzie się poziome okablowanie miedziane z budynku Stacji Karetek Pogotowia Ratunkowego, łącznie 10 lini LAN wykonanych kablem F/FTP kat.6A 500MHz LSOH. Kable miedziane należy zakończyć na panelach krosowych 1U 24-portowych

Do połączenia PD5 z Głównym Punktem Dystrybucyjnym przewidziano szkieletowe połączenie światłowodowe kablem wielomodowym 12-włóknowym 50/125µm OM4 FRNC/LSOH-3. Kabel światłowodowy należy zakończyć w przełącznicy światłowodowej 12xLC (6xLC duplex) metodą spawania.

Szafę 24U należy wyposażyć w:

- 1x przełącznica światłowodowa 1U 24xLC (12xLC duplex) OM4,
- 1x panel krosowy 24-portowy niewyposażony,
- 10x moduł keystone RJ45 kat.6A ekranowany,
- 3x organizator kablowy 1U z wieszakami.

Zasilanie szafy

Dla zasilania szafy PD5 dedykowany obwód zasilający z lokalnej rozdzielni elektrycznej. Dedykowany obwód elektryczny musi zostać zabezpieczony wyłącznikiem różnicowoprądowym i nadprądowym. Szafę należy uziemić.

4.3.3.6 PD6 – Punkt Dystrybucyjny – Portiernia

Punkt Dystrybucyjny okablowania strukturalnego dla budynku Portierni stanowić będzie szafka wisząca 12U, opis szafy punkt 12.8. Szafa serwerowa z wyposażeniem. Lokalizację należy zaplanować w uzgodnieniu z Zamawiającym.

W PD6 schodzić będzie się poziome okablowanie miedziane z Portierni, łącznie 10 linii LAN wykonanych kablem F/FTP kat.6A 500MHz LSOH. Kable miedziane należy zakończyć na panelach krosowych 1U 24-portowych

Do połączenia PD6 z Głównym Punktem Dystrybucyjnym przewidziano szkieletowe połączenie światłowodowe kablem wielomodowym 12-włóknowym 50/125µm OM4 FRNC/LSOH-3. Kabel światłowodowy należy zakończyć w przełącznicy światłowodowej 12xLC (6xLC duplex) metodą spawania.

Szafę 24U należy wyposażyć w:

- 1x przełącznica światłowodowa 1U 24xLC (12xLC duplex) OM4,
- 1x panel krosowy 24-portowy niewyposażony,
- 10x moduł keystone RJ45 kat.6A ekranowany,
- 3x organizator kablowy 1U z wieszakami.

Zasilanie szafy

Dla zasilania szafy PD6 dedykowany obwód zasilający z lokalnej rozdzielni elektrycznej. Dedykowany obwód elektryczny musi zostać zabezpieczony wyłącznikiem różnicowoprądowym i nadprądowym. Szafę należy uziemić.

4.3.3.7 PD7 – Punkt Dystrybucyjny – Izba Przyjęć

Projekt zakłada wykorzystanie istniejącego okablowania strukturalnego w budynku Izby Przyjęć.

W PD7 schodzi się istniejące poziome okablowanie miedziane z budynku Izby Przyjęć, łącznie 28 linii LAN wykonanych kablem cat. 6 UTP TYCO AMP.

Do połączenia PD7 z Głównym Punktem Dystrybucyjnym przewidziano szkieletowe połączenie światłowodowe kablem wielomodowym 12-włóknowym 50/125µm OM4 FRNC/LSOH-3. Kabel światłowodowy należy zakończyć w przełącznicy światłowodowej 12xLC (6xLC duplex) metodą spawania.

Szafę należy doposażyć w:

- 1x przełącznica światłowodowa 1U 24xLC (12xLC duplex) OM4,
- 1x organizator kablowy 1U z wieszakami.

4.3.3.8 – Budynkowy Punkt Dystrybucyjny – Przychodnia Rejonowa w Drzewicy

Projekt zakłada budowę strukturalnej sieci LAN w Przychodni Rejonowej Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Nowym Mieście nad Pilicą w miejscowości Drzewica przy ulicy Stawowej 27.

Punkt Dystrybucyjny okablowania strukturalnego dla budynku Przychodni Rejonowe w Drzewicy stanowić będzie szafka wisząca 18U, opis szafy punkt 12.8. Szafa serwerowa z wyposażeniem. Lokalizację należy zaplanować w uzgodnieniu z Zamawiającym.

W BPD schodzić będzie się poziome okablowanie miedziane z Portierni, łącznie 52 linie LAN wykonanych kablem F/FTP kat.6A 500MHz LSOH. Kable miedziane należy zakończyć na panelach krosowych 1U 24-portowych

Do połączenia BPD Przychodni Rejonowej w Drzewicy z Głównym Punktem Dystrybucyjnym SPZOZ w Nowym Mieście nad Pilicą przewidziano połączenie VPN z wykorzystaniem łączy Internetowych.

Szafę 24U należy wyposażyć w:

- 3x panel krosowy 24-portowy niewyposażony,
- 52x moduł keystone RJ45 kat.6A ekranowany,
- 6x organizator kablowy 1U z wieszakami.

Zasilanie szafy

Dla zasilania szafy BPD dedykowany obwód zasilający z lokalnej rozdzielni elektrycznej. Dedykowany obwód elektryczny musi zostać zabezpieczony wyłącznikiem różnicowoprądowym i nadprądowym. Szafę należy uziemić.

4.3.3.9 – Budynkowy Punkt Dystrybucyjny – Ośrodek Zdrowia w Żdżarach

Projekt zakłada budowę strukturalnej sieci LAN w Ośrodku Zdrowia Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Nowym Mieście nad Pilicą w miejscowości Żdżary 75C.

Punkt Dystrybucyjny okablowania strukturalnego dla budynku Ośrodka Zdrowia w Żdżarach stanowić będzie szafka wisząca 12U, opis szafy punkt 12.8. Szafa serwerowa z wyposażeniem. Lokalizację należy zaplanować w uzgodnieniu z Zamawiającym.

W BPD schodzić będzie się poziome okablowanie miedziane z Ośrodka, łącznie 20 lini LAN wykonanych kablem F/FTP kat.6A 500MHz LSOH. Kable miedziane należy zakończyć na panelach krosowych 1U 24-portowych

Do połączenia BPD Ośrodka Zdrowia w Żdżarach z Głównym Punktem Dystrybucyjnym SPZOZ w Nowym Mieście nad Pilicą przewidziano połączenie VPN z wykorzystaniem łączy Internetowych.

Szafę 24U należy wyposażyć w:

- 1x panel krosowy 24-portowy niewyposażony,
- 20x moduł keystone RJ45 kat.6A ekranowany,
- 3x organizator kablowy 1U z wieszakami.

Zasilanie szafy

Dla zasilania szafy BPD dedykowany obwód zasilający z lokalnej rozdzielni elektrycznej. Dedykowany obwód elektryczny musi zostać zabezpieczony wyłącznikiem różnicowoprądowym i nadprądowym. Szafę należy uziemić.

5. Szczegółowa specyfikacja aktywnych elementów sieci

Na potrzeby stworzenia środowiska informatycznego zgodnego z wcześniej przedstawioną strukturą logiczną, konieczna jest modernizacja sieciowego sprzętu aktywnego poprzez jego wymianę i rozbudowę.
W związku z tym planowany jest zakup niżej wymienionych typów sieciowego sprzętu aktywnego:

- przełącznik szkieletowy/rdzeniowy:
  - wyposażony w możliwość instalacji 24 interfejsów światłowodowych o prędkości transmisji 10Gb/s;
  - wyposażony w 10 portów o prędkości transmisji 10Gb/s (10GBASE-SR);
  - zainstalowany moduł 2 porty 40GbE (QSFP+);
  - obsługa standardu IEEE 802.1Q (VLAN);
  - stakowalny do minimum 10 urządzeń w stosie portami 40GbE;
  - zarządzalny;
- przełącznik dystrybucyjny 24-portowy:
  - co najmniej 24 porty o prędkości transmisji 1Gb/s (1000BASE-T);
  - o co najmniej 2 zintegrowane interfejsy światłowodowe SFP+ o prędkości transmisji 10Gb/s wraz z zamontowaną jedną wkładką światłowodową 10Gb/s odpowiednią do zastosowanego światłowodu;
  - minimum 2 porty do łączenia przełączników w stos;
  - możliwość instalacji drugiego redundantnego zasilacza;
  - obsługa standardu IEEE 802.1Q (VLAN);
  - możliwość połączenia w stos do 12 urządzeń tego samego typu;
  - zarządzalny;
- przełącznik dystrybucyjny 24-portowy PoE:
  - co najmniej 24 porty:
    - ✦ o prędkości transmisji 1Gb/s (1000BASE-T);
    - ✦ obsługujące zasilanie urządzeń w standardzie IEEE 802.3af (PoE) lub 802.3at (PoE+)
  - co najmniej 2 zintegrowane interfejsy światłowodowe SFP+ o prędkości transmisji 10Gb/s wraz z zamontowaną jedną wkładką światłowodową 10Gb/s odpowiednią do zastosowanego światłowodu;
  - minimum 2 porty do łączenia przełączników w stos;
  - możliwość instalacji drugiego redundantnego zasilacza;
  - obsługa standardu IEEE 802.1Q (VLAN);
  - możliwość połączenia w stos do 12 urządzeń tego samego typu
  - zarządzalny;
- przełącznik dystrybucyjny 24-portowy dla potrzeb serwerów:
  - co najmniej 24 porty o prędkości transmisji 1Gb/s (1000BASE-T);
  - o co najmniej 4 interfejsy światłowodowe SFP+ o prędkości transmisji 10Gb/s;

- możliwość dedykowania dwóch portów 10Gb Ethernet SFP+ w celu połączenia przełączników w stos;
- obsługa standardu IEEE 802.1Q (VLAN);
- możliwość połączenia w stos do 4 urządzeń tego samego typu z PoE lub bez;
- zarządzalny;

Każdy switch oprócz podstawowej funkcjonalności, musi prezentować dodatkowe, zaawansowane opcje. Do opcji tych zalicza się:

- zarządzanie jakością pakietów (QoS) - zarządzanie jakością pakietów, czyli QoS oznacza zdolność switche do różnego traktowania poszczególnych ramek. Mając taką funkcję, przełącznik może wykorzystywać ramki o wyższym priorytecie, używając do tego celu oznaczenia znajdującego się w ramkach Ethernet (IEEE 802.1p oraz 802.1Q).
- grupowanie portów - grupowanie (trunk) dwóch lub więcej portów przełącznika pozwala stworzyć jedną logiczną ścieżkę. Ta funkcja umożliwia zwiększenie przepustowości występującej między dwoma przełącznikami.
- VLAN (Virtual Local Area Network) - funkcja VLAN, która pozwala na odizolowanie logiczne grupy urządzeń w ramach współdzielonego medium. Jednocześnie, izolacja ruchu przez porty switche nie pozwala na analizę ruchu w sieci.
- monitoing portów - Funkcja port monitoring umożliwia monitorowanie ruchu na kilku portach przełącznika przez jeden wybrany port.
- redundancja,
- SNMP itp.
- w przypadku rozbudowanych sieci, składających się z wielu połączonych przełączników, niezbędne okażą się mechanizmy zapobiegania awariom (STP, RSTP).

Dodatkowo dla potrzeb sieci bezprzewodowej na terenie budynku Oddziału Szpitalnego planowany jest zakup kontrolera oraz 10 sztuk punktów dostępowych, dedykowanych do zastosowań w szpitalach.

Zaprojektowany kontroler sieci bezprzewodowej to w pełni wyposażony, zintegrowany kontroler dostępu mobilnego, który spełnia wiele wymagań dotyczących mobilnych sieci bezprzewodowych, zabezpieczeń i zdalnego korzystania z sieci.
Zastosowana w nim technologia adaptacyjnego zarządzania drogą radiową dostosowuje sposób interakcji klientów Wi-Fi i sprawdza, czy aplikacje do obsługi transmisji danych, głosu oraz wideo dysponują odpowiednimi zasobami w celu oferowania użytkownikom optymalnego komfortu korzystania z sieci bezprzewodowych.
Pakiet oprogramowania do zarządzania to rozwiązanie, które zarządza infrastrukturą przewodową i bezprzewodową oraz urządzeniami mobilnymi. Łatwy w obsłudze interfejs i podejście ukierunkowane na użytkowników:

- pozwalają wyeliminować konieczność korzystania z wielu specjalistycznych narzędzi administracyjnych,
- umożliwiają określanie priorytetów problemów z łącznością przez dział serwisu,

- umożliwiają inżynierom ds. sieci skupienie się na bardziej strategicznych zadaniach,
- upraszczają egzekwowanie reguł,
- ułatwiają określanie informacji umożliwiających podejmowanie działań w celu planowania przyszłej strategii.

Zaprojektowane punkty dostępu to połączenie mobilnej sieci bezprzewodowej o wysokiej wydajności z dostępem do sieci przewodowej GbE w ramach wyjątkowo kompaktowego, wielofunkcyjnego i przystępnego cenowo urządzenia. Punkt dostępu obsługuje urządzenia klienckie 802.11ac w paśmie 5 GHz z szybkością transmisji danych do 867 Mb/s oraz urządzenia 802.11n w paśmie 2,4 GHz z przepustowością do 400 Mb/s.

W ramach modernizacji sieciowych urządzeń aktywnych konieczne jest wykonanie niżej wymienionych prac:

- wykonanie projektu konfiguracji urządzeń wraz z adresacją sieci LAN, WLAN i zarządzającej;
- konfiguracja i uruchomienie przełączników;
- konfiguracja i uruchomienie kontrolera i punktów dostępowych;
- integracja z innymi systemami;
- stworzenie mapy sieci i dokumentacji powykonawczej.

Przykładowa specyfikacja istotnych warunków zamówienia dla sprzętu

Przełącznik rdzeniowy – światłowodowy

Nazwa komponentu	*Wymagane minimalne parametry techniczne*
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, Głębokość: max 48 cm wraz z kompletem odpowiednich szyn.
Porty	Min 24 porty 10 Gigabit Ethernet SFP+ Zainstalowany moduł 2 porty 40GbE (QSFP+) Możliwość wymiany zainstalowanego modułu min na : - 4 porty 10Gigabit Ethernet SFP+ lub - 4 porty 10Gigabit Ethernet 10GBaseT - 1 port RJ45 umożliwiający zarządzanie poprzez konsolę, - 1 port Ethernet RJ45 dedykowany do zarządzania Out-Of-Band - 1 port USB
Wydajność	Obsługa minimum 4000 wirtualnych sieci Stakowalny do minimum 10 urządzeń w stosie portami 40GbE lub 10GbE (min 160Gbps) Forwarding Rate min. 470 Mpps Switching fabric min. 640 Gbps Rozmiar tablicy routingu min.: 8 000 wpisów IPv4, 4 000 wpisów

	IPv6 Pamięć MAC adresów min. 130 000 ACL – minimum 100 list, minimum 1000 reguł na ACL, min 3000 reguł na wszystkie ACL Bufor pamięci dla pakietów minimum 9 MB Pamięć procesora minimum 2 GB
Funkcjonalność	Musi wspierać funkcjonalność wirtualnej agregacji portów umożliwiającą: • terminowanie pojedynczej wiązki EtherChannel/LACP wyprowadzonej z urządzenia zewnętrznego (serwera, przełącznika) na 2 niezależnych opisywanych urządzeniach • budowę topologii sieci bez pętli z pełnym wykorzystaniem agregowanych łączy • umożliwiać wysokodostępny mechanizm kontroli dla 2 niezależnych opisywanych urządzeń Możliwość obsługi modułów QSFP+ 40GE-SR4 Możliwość obsługi kabli DAC 40GbE i 10GbE (Direct Attached Cable) min długości:: min. 0,5 - 7 m Możliwość obsługi kabli rozszywających DAC (Direct Attached Cable) 1 x 40GbE na 4 x 10GbE min długości: min. 0,5 - 7 m Redundantne min 2 zasilacze AC Redundantne min wiatraki Chłodzenie przełącznika od przodu do tyłu urządzenia Wsparcie dla agregacji LACP (802.3ad) - minimum 128 grup do 8 portów na grupę
Zgodność z protokołami	IEEE 802.1p Traffic Prioritization IEEE 802.1Q VLAN Trunking IEEE 802.1w Rapid Spanning Tree Protocol IEEE 802.1S Multiple Spanning Tree Protocol IEEE 802.1t IEEE802.1D maintenance IEEE 802.1v VLAN Classification by Protocol & Port IEEE 802.1x Port Based Network Access Control IEEE 802.3ac Frame extension for VLAN tags IEEE 802.3x Flow Control IEEE 802.3I IEEE 802.1v VLAN Classification by Protocol & Port IEEE 802.1ab LLDP Obsługa routingu, min.: - RIP v1/2; - OSPF v1/2/3 - VRRP - Policy Based Routing

	- Graceful Restart - BGP Obsługa multicastu, min.: - IGMP v1/2/3; - IGMP Snooping Querier - MLDv2 - PIM-DM - PIM-SM - DHCP - IGMP Proxy
Zarządzanie i bezpieczeństwo	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: - MAC-based authentication - MAC authentication bypass - Guest VLAN Zarządzenie przez CLI i przez przeglądarkę internetową, Radius Radius Accounting RADIUS Tunnel Authentication DHCP options oraz BOOTP vendor extensions Dynamic Host Configuration Protocol (DHCP) klient Bootstrap Protocol DNS Client Form-based File Upload in HTML Simple Network Time Protocol (SNTP) Wsparcie dla IPv6 TLS protocol, version 1.0 PPP Extensible Authentication Protocol, EAP Hypertext Transfer Protocol -- HTTP/1.1 BSD Syslog Protocol Port mirroring Wsparcie dla ramek typu Jumbo 9,000 bajtów Broadcast storm control Możliwośc wgrywania oprogramowania przez USB Trivial File Transfer Protocol (TFTP) Rev. 2

	Honorowanie wartości 802.1p oraz IP DSCP Wsparcie kolejkowania Strict priority oraz algorytmu weighted round robin (WRR) wsparcie dla VLAN ID w ilości 4096 Private VLAN Guest VLAN Locked Port
Komponenty dodatkowe	Wszystkie komponenty muszą pochodzić od tego samego producenta do pozostałe urządzenia sieciowe: 10 modułów SFP+, 10GbE, SR, długość fali 850nm, zasięg 300m
Warunki pracy	Wydajność pracy zasilaczy na poziomie min. 80% Temperatura pracy w zakresie od 0 do 45 stopni Celsjusza Maksymalny pobór mocy 180W 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)
Warunki gwarancji	Pięć lat 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. Gwarancja czasu życia (Limited Lifetime warranty) obejmująca: - przełącznik - zasilacze i wiatraki - moduły SFP, SFP+ i QSFP+ - bezterminowy dostęp do nowych wersji oprogramowania

Przełącznik FC

Nazwa komponentu	*Wymagane minimalne parametry techniczne*
Obudowa	1U z możliwością montażu w szafie rack
Funkcjonalność	• Przełącznik FC musi być wykonany w technologii FC 8 Gb/s i posiadać możliwość pracy portów FC z prędkościami 8, 4, 2, 1 Gb/s z funkcją autonegocjacji prędkości. Wraz z przełącznikiem dostarczyć w sumie 8 szt. kabli światłowodowych lc-lc min. 5 metry. • Przełącznik FC musi posiadać minimum 24 sloty na moduły FC.

	Wszystkie wymagane funkcje muszą być dostępne dla minimum 8 portów FC przełącznika. • Przełącznik musi być dostarczony wraz z minimum 8 modułami SFP FC 8 Gb/s. • Rodzaj obsługiwanych portów: E, F, N oraz FL. • Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) i szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”. • Przełącznik FC musi posiadać nadmiarowe wentylatory N+1. • Przełącznik FC musi być wykonany w tzw. architekturze „non-blocking” uniemożliwiającej blokowanie się ruchu wewnątrz przełącznika przy pełnej prędkości pracy wszystkich portów. • Przełącznik musi posiadać mechanizm balansowania ruchu między grupami połączeń tzw. „trunk” oraz obsługiwać grupy połączeń „trunk” o różnych długościach. • Przełącznik FC musi udostępniać usługę Name Server Zoning - tworzenia stref (zon) w oparciu bazę danych nazw serwerów. • Przełącznik FC musi posiadać możliwość wymiany i aktywacji wersji firmware’u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia, bez wymogu ponownego uruchomienia urządzeń w sieci SAN. • Przełącznik FC musi posiadać wsparcie dla następujących mechanizmów zwiększających poziom bezpieczeństwa: • Listy Kontroli Dostępu definiujące urządzenia (przełączniki i urządzenia końcowe) uprawnione do pracy w sieci Fabric • Możliwość uwierzytelnienia (autentykacji) przełączników z listy kontroli dostępu w sieci Fabric za pomocą protokołów DH-CHAP i FCAP • Możliwość uwierzytelnienia (autentykacji) urządzeń końcowych z listy kontroli dostępu w sieci Fabric za pomocą protokołu DH-CHAP • Kontrola dostępu administracyjnego definiująca możliwość zarządzania przełącznikiem tylko z określonych urządzeń oraz portów • Szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2, • Wskazanie nadrzędnych przełączników odpowiedzialnych za bezpieczeństwo w sieci typu Fabric. • Konta użytkowników definiowane w środowisku RADIUS lub LDAP • Szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS

	• Obsługa SNMP v3 • Przełącznik FC musi posiadać możliwość konfiguracji przez komendy tekstowe w interfejsie znakowym oraz przez przeglądarkę internetową z interfejsem graficznym. • Przełącznik FC musi mieć możliwość instalacji jednomodowych SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 10km. • Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC • Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S v1.1 (powinien zawierać agenta SMI-S zgodnego z wersją standardu v1.1) • Przełącznik FC musi zapewniać możliwość nadawania adresu IP dla zarządzającego portu Ethernet za pomocą protokołu DHCP • Maksymalny dopuszczalny pobór mocy przełącznika FC to 60W • Przełącznik FC musi zapewniać możliwość dynamicznego aktywowania portów za pomocą zakupionych kluczy licencyjnych. • Przełącznik FC musi zapewniać opóźnienie przy przesyłaniu ramek FC między dowolnymi portami nie większe niż 700ns. • Przełącznik FC musi zapewniać sprzętową obsługę zoningu na podstawie portów i adresów WWN • Urządzenie musi wspierać mechanizm balansowania ruchem w połączeniach wewnątrz wielodomenowych sieci fabric w oparciu OXID. • Możliwość wymiany w trybie „na gorąco”: minimum w odniesieniu do modułów portów Fibre Channel (SFP). • Wsparcie dla N_Port ID Virtualization (NPIV). Obsługa co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika.
Wyposażenie	Szyny do montażu w szafie rack.
Gwarancja	Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.

Przełącznik dystrybucyjny 24 portowy

Nazwa komponentu	*Wymagane minimalne parametry techniczne*
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn, wyposażona w zintegrowany zasilacz HotPLUG, możliwość instalacji drugiego redundantnego zasilacza
Porty	Minimum 24 portów GigabitEthernet w standardzie BaseT minimum 2 zintegrowane porty 10Gb Ethernet SFP+, minimum 2 porty do łączenia przełączników w stos, minimum 1 port USB do konfiguracji przełącznika, 1 port RJ45 do portu konsoli wraz z odpowiednim kablem RJ45-RS232.
Wydajność	• minimum 32000 adresów MAC • switch fabric capacity min. 172 Gbps w trybie full-duplex) • forwarding rate min. 128 Mbps • pamięć flash min. 256MB • bufor pamięci dla pakietów minimum 4MB • pamięć procesora minimum 1GB • obsługa minimum 4000 wirtualnych sieci • możliwość połączenia w stos do 12 urządzeń tego samego typu • przepustowości stosu minimum 84 Gbps full duplex • ilość kolejek na port dla ruchu o różnej klasie obsługi: 8 • Wsparcie dla agregacji LACP (802.3ad) - minimum 128 grup do 8 portów na grupę
Zgodność z protokołami	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 Funkcjonalność warstwy 3 : 1058 RIPv1 2453 RIPv2 1724 RIPv2 MIB Extension 2082 RIP-2 MD5 Auth QoS: 2474 DiffServ Field 2697 srTCM 2475 DiffServ Architecture 4115 trTCM
Funkcjonalność	Musi wspierać funkcjonalność wirtualnej agregacji portów umożliwiającą: - terminowanie pojedynczej wiązki EtherChannel/LACP wyprowadzonej z urządzenia zewnętrznego (serwera, przełącznika) na 2 niezależnych opisywanych urządzeniach - budowę topologii sieci bez pętli z pełnym wykorzystaniem agregowanych łączy - umożliwiać wysokodostępny mechanizm kontroli dla 2 niezależnych opisywanych urządzeń
Komponenty dodatkowe	Wszystkie komponenty muszą pochodzić od tego samego producenta do pozostałe urządzenia sieciowe: 1 moduł SFP+, 10GbE, SR, długość fali 850nm, zasięg 300m
Warunki pracy	Wydajność pracy zasilaczy na poziomie min. 80% Temperatura pracy w zakresie od 0 do 45 stopni Celsjusza Maksymalny pobór mocy 120W 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)
Warunki gwarancji	Pięć lat gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 8x65 w dni robocze poprzez ogólnopolską linię telefoniczną producenta. Możliwość rozszerzenia gwarancji producenta do siedmiu lat.

Przełącznik dystrybucyjny 24 portowy PoE

Nazwa komponentu	*Wymagane minimalne parametry techniczne*
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn, wyposażona w zintegrowany zasilacz HotPLUG, możliwość instalacji drugiego redundantnego zasilacza zapewniającego 1000W mocy
Porty	Minimum 24 portów GigabitEthernet w standardzie BaseT PoE+ minimum 2 zintegrowane porty 10Gb Ethernet SFP+, minimum 2 porty do łączenia przełączników w stos, minimum 1 port USB do konfiguracji przełącznika, 1 port RJ45 do portu konsoli wraz z odpowiednim kablem RJ45-RS232. Dostępny budżet mocy PoE na portach: 850W
Wydajność	• minimum 32000 adresów MAC • switch fabric capacity min. 172 Gbps w trybie full-duplex) • forwarding rate min. 128 Mbps • pamięć flash min. 256MB • bufor pamięci dla pakietów minimum 4MB • pamięć procesora minimum 1GB • obsługa minimum 4000 wirtualnych sieci • możliwość połączenia w stos do 12 urządzeń tego samego typu • przepustowości stosu minimum 84 Gbps full duplex • ilość kolejek na port dla ruchu o różnej klasie obsługi: 8 • Wsparcie dla agregacji LACP (802.3ad) - minimum 128 grup do 8 portów na grupę
Zgodność z protokołami	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 Funkcjonalność warstwy 3 : 1058 RIPv1 2453 RIPv2 1724 RIPv2 MIB Extension 2082 RIP-2 MD5 Auth QoS: 2474 DiffServ Field 2697 srTCM 2475 DiffServ Architecture 4115 trTCM
Funkcjonalność	Musi wspierać funkcjonalność wirtualnej agregacji portów umożliwiającą: - terminowanie pojedynczej wiązki EtherChannel/LACP wyprowadzonej z urządzenia zewnętrznego (serwera, przełącznika) na 2 niezależnych opisywanych urządzeniach - budowę topologii sieci bez pętli z pełnym wykorzystaniem agregowanych łączy - umożliwiać wysokodostępny mechanizm kontroli dla 2 niezależnych opisywanych urządzeń
Komponenty dodatkowe	Wszystkie komponenty muszą pochodzić od tego samego producenta do pozostałe urządzenia sieciowe: 1 moduł SFP+, 10GbE, SR, długość fali 850nm, zasięg 300m
Warunki pracy	Wydajność pracy zasilaczy na poziomie min. 80% Temperatura pracy w zakresie od 0 do 45 stopni Celsjusza Maksymalny pobór mocy 1050W 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)
Warunki gwarancji	Pięć lat gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji następnego dnia roboczego od przyjęcia zgłoszenia,

	możliwość zgłaszania awarii w trybie 8x5 w dni robocze poprzez ogólnopolską linię telefoniczną producenta. Możliwość rozszerzenia gwarancji producenta do siedmiu lat.

Przełącznik dystrybucyjny 24 portowy dla potrzeb serwerów

Nazwa komponentu	*Wymagane minimalne parametry techniczne*
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn, wyposażona w zintegrowany zasilacz o mocy nie przekraczającej 40W
Porty	Minimum 24 porty GigabitEthernet w standardzie BaseT, 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.
Wydajność	• Minimum 16000 adresów MAC • switch fabric capacity min. 128Gbps w trybie full-duplex • forwarding rate min. 128Mbps • 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 4 urządzeń tego samego typu z PoE lub bez
Zgodność z protokołami	Prędkość przełączania Wirespeed dla każdego portu 1GE oraz 10 Gb DHCP-snooping, DHCP Relay Agent Dynamic-ARP protection 802.1AB LLDP 802.1p Ethernet Priority (User Provisioning and Mapping) 802.1Q VLAN Tagging, Double VLAN Tagging, GVRP 802.1v Protocol-based VLANs BPDU guard, BPDU filtering 802.2 Logical Link Control 802.3ac Frame Extensions for VLAN Tagging 802.3AX LAG Load Balancing 802.3az Energy Efficient Ethernet (EEE) 802.3x Flow Control

	ANSI LLDP-MED (TIA-1057) MTU 9,216 byte
Funkcjonalność Ethernet dla warstwy 2	Trunking IEEE 802.1Q VLAN 802.1D Bridging, Spanning Tree 802.1W Rapid Spanning Tree (RSTP) Rapid Per-VLAN Spanning Tree (IEEE 802.1w) Wsparcie dla PVST+ Multiple Spanning Tree Protocol (MSTP) (IEEE 802.1s) SpanningTree Root Guard Link Aggregation Control Protocol (LACP): IEEE 802.3ad Grupowanie EtherChannel/ LACP (min liczka grup: 64, ilość portów per wiązka: 8 Ramki Jumbo dla wszystkich portów (do 9 000 bajtów) Prewencja niekontrolowanego wzrostu ilości ruchu (stormcontrol), dla ruchu unicast, multicast, broadcast
Funkcje QoS	Layer 2 IEEE 802.1p (CoS) 8 sprzętowych kolejek per port Klasyfikacja QoS w oparciu o listy (ACL (Access control list) w warstwach 2, 3, 4 Kolejkowanie na wyjściu w oparciu o CoS Bezwzględne (strict-priority) kolejkowanie na wyjściu Kolejkowanie WRR (WeightedRound-Robin) na wyjściu DiffServ Field DiffServ Architecture Assured Fwd PHB Port Based QoS
Funkcje bezpieczeństwa	Wejściowe ACL (standardowe oraz rozszerzone) Standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC addresses, typ protokołu Standardowe oraz rozszerzone ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i v6 ilość reguł ACL per system min 2 000 ACL oparte o parametr czasu ACL oparte o porty (PACL) Logowanie i statystyka dla ACL SSHv2 4251 SSHv2 Protocol 4252 SSHv2 Authentication 4253 SSHv2 Transport 4254 SSHv2 Connection Protocol 4419 SSHv2 Transport Layer Protocol Authentication, authorization, and accounting (AAA) 2865 RADIUS 2866 RADIUS Accounting 2868 RADIUS Attributes for Tunnel Prot. 2869 RADIUS Extensions 802.1X Network Access Control, Auto VLAN

Funkcje zarządzania	Port zarządzający 10/100/1000 Mbps Port konsoli CLI Telnet TACACS+ Syslog SNMP v1, v2, v3 Enhanced SNMP MIB Remote monitoring (RMON) Role Based Access Control (RBAC) SFLOW lub równoważny Kopiowanie ruchu za pośrednictwem mechanizmu Switched Port Analyzer (RSPAN) lub równoważny dla fizycznych portów Ethernet, wiązek PortChannel/LACP, interfejsów VLAN Liczniki pakietów wchodzących/wychodzących per każdy port Simple Network Time Protocol (SNTP) Diagnostyka procesu boot 4521 LDAP Extensions 4716 SECSH Public Key File Format
Komponenty dodatkowe	Wszystkie komponenty muszą pochodzić od tego samego producenta do pozostałe urządzenia sieciowe: 1 moduł SFP+, 10GbE, SR, długość fali 850nm, zasięg 300m
Funkcjonalność Ethernet dla warstwy 3	Minimum: RIP v.2
Funkcje obsługi Multicastów	Minimum: IGMP v1/v2/v3 Snooping & Querier
Warunki gwarancji	Pięć lat 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.

Kontroler sieci bezprzewodowej

Nazwa komponentu	*Wymagane minimalne parametry techniczne*
Obudowa	Rack maksymalnie 1U
Porty	• Posiada co najmniej cztery interfejsy podwójnego zastosowania 10/100/1000Base-T RJ45 wymiennie z 1000Base-X SFP. • Wbudowany port RJ45 konsoli szeregowej RS-232.

Obsługa AP	• Umożliwia obsługę co najmniej 10 bezprzewodowych punktów dostępowych w chwili dostawy z możliwością licencyjnej rozbudowy do co najmniej 132 podłączonych za pomocą LAN.
Wydajność oprogramowania kontrolera	• Punkty dostępu połączone z siecią LAN (maks.) - 32 • Zdalne punkty dostępu (maks.) - 128 • Użytkownicy (maks.) - 2048 • Adresy MAC - 64 000 • Interfejsy IP sieci VLAN - 256 • Liczba tras unicast protokołu IPv4 - 2048 • Aktywne sesje zapory sieciowej - 128 000 • Równoczesne tunele IPsec (maks.) - 2048 • Systemowe identyfikatory BSSID - 256 • Przepustowość zapory sieciowej - 3 Gb/s • Przepustowość przy szyfrowaniu (3DES, AESCBC256) - 1,6 Gb/s • Przepustowość przy szyfrowaniu (AES-CCM) - 0,8 Gb/s
Pozostałe funkcjonalności	• Możliwość licencyjnego uruchomienia usługi zaawansowanego szyfrowania klasy Suite B z wykorzystaniem algorytmów AES-128-GCM oraz AES-256-GCM ze wsparciem sprzętowym szyfrowania. • Możliwość licencyjnego uruchomienia usług wykrywania, przeciwdziałania i zwalczania zagrożeń w sieci bezprzewodowej (intrusion prevention) takich jak wykrywania sieci ad-hoc, podszywania się, ataków WEP, fałszowania ramek kontrolnych. • Wsparcie dla bezpiecznego uwierzytelniania bezprzewodowych punktów dostępowych na kontrolerze z wykorzystaniem certyfikatów. • Możliwość definiowania list „zaufanych” punktów dostępowych. • Obsługa list dostępu ACL standardowych i rozszerzonych. • Klasyfikacja portów fizycznych i logicznych (VLAN) jako zaufane oraz niezaufane. • Możliwość budowania reguł przypisania do sieci VLAN na podstawie roli użytkownika, typu autentykacji, RADIUS oraz 802.1X. • Uwierzytelnianie użytkowników oraz urządzeń w oparciu o wewnętrzną bazę oraz RADIUS (wliczając VSA), LDAP, TACACS+ i (NTLM). • Uwierzytelnianie użytkowników w oparciu o Captive Portal bezpośrednio na kontrolerze oraz obsługa zewnętrznych Captive Portali. • Obsługa uwierzytelniania 802.1X przy wykorzystaniu EAP-PEAP, EAP-TLS, EAP-TTLS, EAP-GTC EAP-MD5, EAP-FAST, EAP-MSCHAPv2.

	• Możliwość powiększania pojemności oraz podnoszenia ciągłości pracy infrastruktury sieci bezprzewodowej, poprzez tworzenie klastrów kontrolerów z wyznaczeniem ról kontrolera nadrzędnego (master) i podrzędnego (local), gdzie kontroler nadrzędny (master) definiuje ustawienia security i radiowe dla całej sieci. Komunikacja pomiędzy kontrolerami powinna być szyfrowana w oparciu o protokół IPSec (hasło/klucz, certyfikaty). • Wsparcie dla mechanizmu wysokiej dostępności dzięki któremu, punkt dostępowy utrzymuje dwa połączenia, jedno z kontrolerem aktywnym, drugie z kontrolerem zapasowych, umożliwiające szybkie przełączenie na kontroler zapasowy w przypadku awarii bądź utraty łączności z kontrolerem aktywnym, bez konieczności restartu punktu dostępowego. Mechanizm powinien wspierać scenariusze active/active, 1:1 oraz N:1. • Posiadający mechanizm optymalizujący pracę całego rozwiązania WLAN (pojedynczy punkt dostępowy, klaster lub infrastruktura zarządzana przez kontroler) automatycznie gospodarujący zasobami radiowymi w zakresie najlepszego wyboru kanału i mocy nadawania dla każdego punktu dostępowego z osobna. • Obsługa IP Mobility. • Wsparcie funkcjonalności łączonych sieci VLAN, tzw. vlan pooling. • Możliwość konfiguracji urządzenia poprzez konsolę szeregową, SSH, telnet, interfejs web, dedykowany system NMS producenta urządzenia oraz przy pomocy kreatorów zagnieżdżonych w oprogramowaniu urządzenia.
Gwarancja	Pięć lat gwarancji realizowanej w miejscu instalacji sprzętu, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Możliwość rozszerzenia gwarancji producenta do siedmiu lat.

Punkt dostępowy sieci bezprzewodowej

Nazwa komponentu	*Wymagane minimalne parametry techniczne*
Standard	Minimum dwuradiowy pracujący w standardzie IEEE 802.11a/b/g/n/ac;
SSID	Obsługa min. 16 SSID na radio

Zasilanie	Zasilanie poprzez skrętkę (PoE) zgodne z IEEE 802.3af Pobór mocy max 13Watt
Interfejsy	Min. 3 x GbE 2 x Pass-through Port konsolowy RJ-45 USB host interface
Kontroler	Punkt dostępowy współpracujący z kontrolerem i konsolą zarządzającą będącymi przedmiotem przetargu pochodzący od tego samego producenta
Pasmo/ Częstotliwość	praca w paśmie 2,4 GHz i 5 GHz
Tryb pracy	Praca w trybie MIMO 2x2:2
Funkcjonalności	Wbudowana funkcjonalność analizatora spektrum pasma m.in.: w celu identyfikacji źródeł interferencji, Wspierane modulacje: BPSK, QPSK, CCK, 16-QAM, 64-QAM
Anteny	Anteny wbudowane i zintegrowane z punktem dostępowym
Zarządzanie	Zarządzanie wykorzystywanymi kanałami radiowymi oraz mocą sygnału z poziomu kontrolera
Gwarancja	Gwarancja dożywotnia obejmująca sprzęt, możliwość zgłaszania awarii w trybie 8x5 w dni robocze poprzez ogólnopolską linię telefoniczną producenta.

Punkt styku z siecią (UTM, router) – budynek główny

Nazwa komponentu	***Wymagane minimalne parametry techniczne***
Typ urządzenia	Urządzenie typu UTM, zapewniające funkcjonalności: Firewall, Koncentrator IPSec VPN, ochrona przed wirusami, spyware, sonda IPS, filtrowanie poczty, filtrowanie stron www po kategoriach i według reguł tworzonych przez administratora
Specyfikacja fizyczna urządzenia	a. Dedykowane rozwiązanie sprzętowe b. Obudowa 1U przeznaczona do montażu w szafie RACK c. Pamięć RAM: minimum 2 GB d. Procesor wielordzeniowy: 4x 800 MHz e. Ilość interfejsów: i. Nie mniej niż 8 interfejsów GigabitEthernet ii. Nie mniej niż 2 interfejsy USB iii. 1 interfejs konsoli iv. 1 interfejs zarządzania v. Gniazdo rozszerzeń

Wydajność urządzenia	a. Obsługa nielimitowanej ilości hostów w sieci chronionej b. Przepustowość zapory sieciowej przy pracy w trybie Statefull Packet Inspection, mierzona zgodnie z zaleceniami RFC 2544: nie mniejsza niż 1,9 Gbps c. Przepustowość zapory sieciowej pracującej jako sonda IPS, mierzona zgodnie z zaleceniami RFC 2544: nie mniejsza niż 700 Mbps d. Przepustowość zapory sieciowej przy pracy w trybie Deep Packet Inspection, przy włączonych wszystkich usługach filtrowania i skanowania: nie mniejsza niż 300 Mbps e. Przepustowość zintegrowanego z zaporą sieciową koncentratora połączeń IPSec VPN AES/3DES mierzona zgodnie z zaleceniami RFC 2544: nie mniejsza niż 1,1 Gbps f. Maksymalna ilość jednocześnie obsługiwanych sesji: nie mniej niż 225000 g. Obsługa nie mniej niż 15000 nowych sesji na sekundę b. Ochrona przed atakami DoS i DDoS
Funkcjonalności urządzenia w zakresie konfiguracji połączeń IPSec VPN	a. Minimalna ilość jednocześnie obsługiwanych połączeń IPSec VPN: 75 b. Minimalna ilość klientów IPSec VPN w cenie urządzenia: 10 c. Wspierane mechanizmy uwierzytelniania i szyfrowania: DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1 d. Wspierane mechanizmy wymiany kluczy: IKE, IKEv2, Manual Key, PKI (X.509) e. Wsparcie certyfikatów: Verisign, Thawte, Cybertrust, RSA Keon, Entrust, Microsoft CA dla połączeń site-to-site pomiędzy urządzeniami UTM f. Obsługa funkcjonalności: L2TP IPSec, DHCP over VPN, redundantna brama zdalna w przypadku połączeń site-site VPN
Sieciowe funkcjonalności urządzenia	a. Możliwość pracy jako Router, Bridge L2 lub w trybie transparentnym b. Obsługa nie mniej niż 50 sieci VLAN działających zgodnie ze standardem 802.1Q c. Wbudowany serwer DHCP umożliwiający przydzielanie adresów statycznie, dynamicznie, przekierowanie zgłoszeń do zewnętrznego serwera DHCP d. Możliwość przesyłania komunikatów DHCP pomiędzy różnymi strefami e. Wsparcie mechanizmów NAT: 1:1, 1:many, many:1, many:many, PAT f. Możliwość scentralizowanego zarządzania nie mniej niż

	32 punktami dostępowymi, wsparcie dla standardów 802.11 b/g/n, WEP, WPA, WPA2, TKIP, 802.1x, EAP-PEAP, g. EAP-TTLS, IPSec over WLAN h. Możliwość kreowania reguł routingu statycznego i. Wsparcie dynamicznych protokołów routingu: BGP, RIP v1/v2, OSPF i wsparcie dla routowania transmisji multicast j. Wsparcie funkcjonalności QoS: tagowanie/mapowanie 802.1p, DSCP, możliwość ustawienia przynajmniej 100 reguł określających maksymalne i gwarantowane pasmo k. Możliwość skonfigurowania przynajmniej 2 łączy WAN, działających w trybie redundantnym lub umożliwiających równoważenie obciążeń dla ruchu wychodzącego. l. Możliwość konfiguracji monitorowania pracy łączy WAN w oparciu o połączenia TCP i ICMP i reguł przełączenia ruchu z łącza podstawowego na łącze redundantne m. Możliwość konfiguracji reguł równoważenia obciążeń dla ruchu przychodzącego do hostów znajdujących się w sieci chronionej n. Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń, pełna kompatybilność z większością urządzeń i serwerów VoIP
Funkcjonalności urządzenia w zakresie uwierzytelniania użytkowników	a. Lokalna baza użytkowników b. Uwierzytelnianie użytkowników w oparciu o: XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, Terminal Services, Citrix
Funkcjonalności urządzenia w zakresie zarządzania i wysokiej dostępności	a. Możliwość zarządzania urządzeniem poprzez: HTTP, HTTPS, CLI (SSH, konsola), SNMP b. Możliwość dokupienia dedykowanego oprogramowania do scentralizowanego zarządzania większą ilością urządzeń c. Możliwość podłączenia drugiego urządzenia do pracy w klastrze wysokiej dostępności w trybie Active – Passive z synchronizacją sesji, lub opcjonalnie w trybie Active – Active
Funkcjonalności urządzenia w zakresie mechanizmów filtrowania Deep Packet Inspection i Statefull Packet Inspection	a. Możliwość kreowania stref bezpieczeństwa przydzielanych do danych interfejsów zarówno fizycznych, jak i wirtualnych (możliwość przypisania więcej niż jednego interfejsu do pojedynczej strefy bezpieczeństwa) b. Możliwość indywidualnej konfiguracji usług bezpieczeństwa dla każdej ze stref c. Możliwość kreowania reguł Firewall dla ruchu

przychodzącego/wychodzącego z/do zadanej strefy, w określonych przedziałach czasu, z uwzględnieniem użytkowników, dla których reguła ma być aktywna

d. Możliwość włączania i wyłączania reguł Firewall i NAT bez konieczności ich usuwania
e. Wymagane jest, aby na urządzeniu uruchomione były następujące usługi w subskrypcji na okres 36 miesięcy:
    i. Sieciowa ochrona antywirusowa zapewniająca skanowanie ruchu na protokołach HTTP, FTP, POP3, SMTP, IMAP, ruch TCP oraz NetBios.
    ii. Filtr antywirusowy powinien zapewniać skanowanie załączników poczty elektronicznej, plików skompresowanych ZIP i GZIP. Wymagane jest, aby możliwe było włączenie lub wyłączenie usługi antywirus w poszczególnych strefach bezpieczeństwa, oraz możliwość włączenia lub wyłączenia reagowania na określone sygnatury.
    iii. Sonda IDP (detekcja i blokowanie wtargnięć do sieci) zapewniająca skanowanie ruchu w oparciu o sygnatury dostarczone przez producenta. Sygnatury powinny umożliwiać wykrywanie i blokowanie zdarzeń takich jak: korzystanie z programów do wymiany plików P2P (np. Limewire, BitTorrent, eMule, etc.), korzystanie z komunikatorów internetowych (np. Yahoo Messenger, Gadu-Gadu, Skype, etc.), ataki typu backdoor, exploit, SQL-Injection, etc. Wymagane jest, aby poza możliwością włączenia lub wyłączenia usługi IDP w poszczególnych strefach bezpieczeństwa możliwa była indywidualna konfiguracja każdej z sygnatur w celu uruchomienia bądź wyłączenia jej dla zadanych adresów IP, użytkowników lub przedziałów czasowych.
    iv. Sieciowa ochrona antyspyware, zapewniająca skanowanie ruchu HTTP, FTP, SMTP, POP3, IMAP. Wymagane jest, aby poza możliwością włączenia lub wyłączenia usługi IDP w poszczególnych strefach bezpieczeństwa możliwa była indywidualna konfiguracja każdej z sygnatur w celu uruchomienia bądź wyłączenia jej dla zadanych adresów IP, użytkowników lub przedziałów czasowych.

	v. Usługa filtrowania treści stron WWW, zapewniająca blokowanie apletów Java, aplikacji Active-X, plików cookie, definiowanie białych i czarnych list stron www, definiowanie słów kluczowych umożliwiających zablokowanie strony w przypadku ich wystąpienia. Dodatkowo wymagane jest tworzenie reguł filtrowania treści dla poszczególnych grup użytkowników umożliwiających filtrowanie treści w oparciu o informacje z zewnętrznych serwerów zawierających bazę stron zestawionych w co najmniej 56 kategoriach. Wymagane jest, aby mechanizm filtrowania treści uwzględniał także filtrowanie stron HTTPS oraz możliwość włączenia lub wyłączenia mechanizmu filtrowania treści w poszczególnych strefach bezpieczeństwa i zdefiniowanie domyślnej reguły dla każdej ze stref działającej niezależnie od uprawnień poszczególnych użytkowników. vi. Usługa Firewall aplikacji umożliwiająca definiowanie własnych sygnatur oraz reakcji urządzenia w przypadku wykrycia ruchu zgodnego z wprowadzonymi sygnaturami. vii. Ochrona poczty elektronicznej w oparciu o białe/czarne listy nadawców oraz serwery RBL. f. Wymagana jest taka możliwość skonfigurowania połączeń IPSec VPN client-site, aby cały ruch z połączonych do urządzenia klientów był przesyłany poprzez urządzenie i możliwe było jego skanowanie przez mechanizmy antywirus, antyspyware, IDP, filtrowania treści. g. Wymaga się, aby na urządzeniu możliwe było włączenie blokowania ruchu przesyłanego pomiędzy strefami w przypadku, kiedy na stacjach roboczych lub serwerach nie ma zainstalowanego odpowiedniego oprogramowania antywirusowego, lub oprogramowanie to będzie miało nieaktualne sygnatury. h. Wymaga się, aby mechanizmy antywirus, antyspyware i sonda IDP nie posiadały ograniczeń co do wielkości skanowanych plików
Monitorowanie i raportowanie zdarzeń	a. Wymagane jest dostarczenie dedykowanego oprogramowania (instalowanego na zewnętrznym serwerze) zapewniającego monitorowanie, rejestrację i

	graficzną (w postaci tabel i wykresów) prezentację danych przesłanych z urządzenia firewall dotyczących ruchu, oraz zagrożeń sieciowych. Niezbędne dane to średnia zajętość łącza w podziale na dni i godziny, wykorzystanie pasma przez każdego z użytkowników, informacje dotyczące przeglądanych witryn przez każdego z użytkowników sieci informatycznej, informacje dotyczące użytkowników łamiących zasady przeglądania witryn, informacje dot. ataków, detekcji intruzów, zagrożeń antywirusowych. Dane muszą mieć możliwość wydruku. b. Oprogramowanie winno posiadać funkcjonalność tworzenia raportów opartych o własne reguły z możliwością przechodzenia w wyznaczone obszary raportu i obrazowania ich w bardziej szczegółowy sposób.
Wsparcie techniczne i gwarancja	Wymagane jest aby dostarczane urządzenie objęte było okresem gwarancji przez okres 36 miesięcy, z możliwością przedłużenia na dłuższy okres czasu.

Punkt styku z siecią (UTM, router) – oddziały

Nazwa komponentu	*Wymagane minimalne parametry techniczne*
Typ urządzenia	Urządzenie typu UTM, zapewniające funkcjonalności: Firewall, Koncentrator IPSec VPN, ochrona przed wirusami, spyware, sonda IPS, filtrowanie stron www po kategoriach i według reguł tworzonych przez administratora
Specyfikacja fizyczna urządzenia	1. Obudowa 1U przeznaczona do montażu w szafie RACK 2. Pamięć RAM: minimum 1GB 3. Procesor wielordzeniowy: 2x800MHz 4. Ilość interfejsów: a. Nie mniej niż 5 interfejsów GigabitEthernet b. Nie mniej niż 1 interfejs USB
Wydajność urządzenia	1. Obsługa nielimitowanej ilości hostów w sieci chronionej 2. Przepustowość zapory sieciowej przy pracy w trybie Statefull Packet Inspection, mierzona zgodnie z zaleceniami RFC 2544: nie mniejsza niż 740 Mbps 3. Przepustowość zapory sieciowej pracującej jako sonda IPS, mierzona zgodnie z zaleceniami RFC 2544: nie mniejsza niż 300 Mbps 4. Przepustowość zapory sieciowej przy pracy w trybie Deep Packet Inspection, przy włączonych wszystkich usługach filtrowania i skanowania: nie mniejsza niż 40 Mbps 5. Przepustowość zintegrowanego z zaporą sieciową koncentratora połączeń IPSec VPN AES/3DES mierzona zgodnie

	z zaleceniami RFC 2544: nie mniejsza niż 290 Mbps 6. Maksymalna ilość jednocześnie obsługiwanych sesji: nie mniej niż 50 000 7. Obsługa nie mniej niż 5 000 nowych sesji na sekundę 8. Ochrona przed atakami DoS i DDoS
Funkcjonalności urządzenia w zakresie konfiguracji połączeń IPSec VPN	1. Minimalna ilość jednocześnie obsługiwanych połączeń IPSec VPN: 10 2. Minimalna ilość klientów IPSec VPN w cenie urządzenia: 1 3. Wspierane mechanizmy uwierzytelniania i szyfrowania: DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1 4. Wspierane mechanizmy wymiany kluczy: 5. IKE, IKEv2, Manual Key, PKI (X.509) 6. Wsparcie certyfikatów: 7. Verisign, Thawte, Cybertrust, RSA Keon, Entrust, Microsoft CA dla połączeń site-to-site pomiędzy urządzeniami UTM 8. Obsługa funkcjonalności: L2TP IPSec, DHCP over VPN, redundantna brama zdalna w przypadku połączeń site-site VPN
Sieciowe funkcjonalności urządzenia	1. Możliwość pracy jako Router, Bridge L2 lub w trybie transparentnym 2. Obsługa nie mniej niż 25 sieci VLAN działających zgodnie ze standardem 802.1Q 3. Wbudowany serwer DHCP umożliwiający przydzielanie adresów statycznie, dynamicznie, przekierowanie zgłoszeń do zewnętrznego serwera DHCP 4. Możliwość przesyłania komunikatów DHCP pomiędzy różnymi strefami 5. Wsparcie mechanizmów NAT: 1:1, 1:many, many:1, many:many, PAT 6. Możliwość scentralizowanego zarządzania nie mniej niż 16 punktami dostępowymi, wsparcie dla standardów 802.11 b/g/n, WEP, WPA, WPA2, TKIP, 802.1x, EAP-PEAP, EAP-TTLS, IPSec over WLAN 7. Możliwość kreowania reguł routingu statycznego 8. Wsparcie dynamicznych protokołów routingu: BGP, RIP v1/v2, OSPF i wsparcie dla routowania transmisji multicast 9. Wsparcie funkcjonalności QoS: tagowanie/mapowanie 802.1p, DSCP, możliwość ustawienia przynajmniej 100 reguł określających maksymalne i gwarantowane pasmo 10. Możliwość skonfigurowania przynajmniej 2 łączy WAN, działających w trybie redundantnym lub umożliwiających równoważenie obciążeń dla ruchu wychodzącego. 11. Możliwość konfiguracji monitorowania pracy łączy WAN w oparciu o połączenia TCP i ICMP i reguł przełączenia ruchu z łącza podstawowego na łącze redundantne 12. Możliwość konfiguracji reguł równoważenia obciążeń dla ruchu przychodzącego do hostów znajdujących się w sieci chronionej

	13. Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń, pełna kompatybilność z większością urządzeń i serwerów VoIP
Funkcjonalności urządzenia w zakresie uwierzytelniania użytkowników	1. Lokalna baza użytkowników 2. Uwierzytelnianie użytkowników w oparciu o: XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, Terminal Services, Citrix
Funkcjonalności urządzenia w zakresie zarządzania i wysokiej dostępności	1. Możliwość zarządzania urządzeniem poprzez: HTTP, HTTPS, CLI (SSH, konsola), SNMP 2. Możliwość dokupienia dedykowanego oprogramowania do scentralizowanego zarządzania większą ilością urządzeń 3. Możliwość podłączenia drugiego urządzenia do pracy w klastrze wysokiej dostępności w trybie Active – Standby
Funkcjonalności urządzenia w zakresie mechanizmów filtrowania Deep Packet Inspection i Statefull Packet Inspection	1. Możliwość kreowania stref bezpieczeństwa przydzielanych do danych interfejsów zarówno fizycznych, jak i wirtualnych (możliwość przypisania więcej niż jednego interfejsu do pojedynczej strefy bezpieczeństwa) 2. Możliwość indywidualnej konfiguracji usług bezpieczeństwa dla każdej ze stref 3. Możliwość kreowania reguł Firewall dla ruchu przychodzącego/wychodzącego z/do zadanej strefy, w określonych przedziałach czasu, z uwzględnieniem użytkowników, dla których reguła ma być aktywna 4. Możliwość włączania i wyłączania reguł Firewall i NAT bez konieczności ich usuwania 5. Wymagane jest, aby na urządzeniu uruchomione były następujące usługi w subskrypcji na okres 36 miesięcy: – Sieciowa ochrona antywirusowa zapewniająca skanowanie ruchu na protokołach HTTP, FTP, POP3, SMTP, IMAP, ruch TCP oraz NetBios. – Filtr antywirusowy powinien zapewniać skanowanie załączników poczty elektronicznej, plików skompresowanych ZIP i GZIP. Wymagane jest, aby możliwe było włączenie lub wyłączenie usługi antywirus w poszczególnych strefach bezpieczeństwa, oraz możliwość włączenia lub wyłączenia reagowania na określone sygnatury. – Sonda IDP (detekcja i blokowanie wtargnięć do sieci) zapewniająca skanowanie ruchu w oparciu o sygnatury dostarczone przez producenta. Sygnatury powinny umożliwiać wykrywanie i blokowanie zdarzeń takich jak: korzystanie z programów do wymiany plików P2P (np. Limewire, BitTorrent, eMule, etc.), korzystanie z komunikatorów internetowych (np. Yahoo Messenger,

	Gadu-Gadu, Skype, etc.), ataki typu backdoor, exploit, SQL-Injection, etc. Wymagane jest, aby poza możliwością włączenia lub wyłączenia usługi IDP w poszczególnych strefach bezpieczeństwa możliwa była indywidualna konfiguracja każdej z sygnatur w celu uruchomienia bądź wyłączenia jej dla zadanych adresów IP, użytkowników lub przedziałów czasowych. – Sieciowa ochrona antyspyware, zapewniająca skanowanie ruchu HTTP, FTP, SMTP, POP3, IMAP. Wymagane jest, aby poza możliwością włączenia lub wyłączenia usługi IDP w poszczególnych strefach bezpieczeństwa możliwa była indywidualna konfiguracja każdej z sygnatur w celu uruchomienia bądź wyłączenia jej dla zadanych adresów IP, użytkowników lub przedziałów czasowych. – Usługa filtrowania treści stron WWW, zapewniająca blokowanie apletów Java, aplikacji Active-X, plików cookie, definiowanie białych i czarnych list stron www, definiowanie słów kluczowych umożliwiających zablokowanie strony w przypadku ich wystąpienia. Dodatkowo wymagane jest tworzenie reguł filtrowania treści dla poszczególnych grup użytkowników umożliwiających filtrowanie treści w oparciu o informacje z zewnętrznych serwerów zawierających bazę stron zestawionych w co najmniej 56 kategoriach. Wymagane jest, aby mechanizm filtrowania treści uwzględniał także filtrowanie stron HTTPS oraz możliwość włączenia lub wyłączenia mechanizmu filtrowania treści w poszczególnych strefach bezpieczeństwa i zdefiniowanie domyślnej reguły dla każdej ze stref działającej niezależnie od uprawnień poszczególnych użytkowników. – Usługa Firewall aplikacji umożliwiająca definiowanie własnych sygnatur oraz reakcji urządzenia w przypadku wykrycia ruchu zgodnego z wprowadzonymi sygnaturami. – Ochrona poczty elektronicznej w oparciu o białe/czarne listy nadawców oraz serwery RBL. 6. Wymagana jest taka możliwość skonfigurowania połączeń IPSec VPN client-site, aby cały ruch z połączonych do urządzenia klientów był przesyłany poprzez urządzenie i możliwe było jego skanowanie przez mechanizmy antywirus, antyspyware, IDP, filtrowania treści. 7. Wymaga się, aby na urządzeniu możliwe było włączenie blokowania ruchu przesyłanego pomiędzy strefami w przypadku, kiedy na stacjach roboczych lub serwerach nie ma zainstalowanego odpowiedniego oprogramowania antywirusowego, lub oprogramowanie to będzie miało nieaktualne sygnatury. 8. Wymaga się, aby mechanizmy antywirus, antyspyware i sonda

	IDP nie posiadały ograniczeń co do wielkości skanowanych plików
Wsparcie techniczne i gwarancja	Wymagane jest aby dostarczane urządzenie objęte było okresem gwarancji przez okres 36 miesięcy, z możliwością przedłużenia na dłuższy okres czasu.

Oprogramowanie do monitorowania

Nazwa komponentu	*Wymagane minimalne parametry techniczne*
Przeznaczenie	Rozwiązanie do monitorowania krytycznych zdarzeń i aktywności sieciowej takich jak zagrożenia sieciowe, niestosowne wykorzystanie zasobów Webowych, poziom wykorzystania pasma. Rozwiązanie dostarcza szczegółowe i wyczerpujące raporty na temat aktywności sieciowej. Moduł raportujący jest aplikacją tworzącą dynamiczne raporty Webowe, które mogą dotyczyć zarówno zdarzeń czasu rzeczywistego jak i raportów historycznych kompletny wgląd w aktywność sieciową na dostarczonym urządzeniu bezpieczeństwa. Raportowanie pozwala na monitorowanie sieci, zwiększenie bezpieczeństwa poprzez zapewnienie wglądu w zdarzenia na urządzeniu oraz przewidywanie przyszłego zapotrzebowania na pasmo. Baza danych systemu w najnowszej wersji to MySQL. Dostęp do rozwiązania poprzez interfejs webowy. System ma wydzielone dwa interfejsy: • interfejs zarządzania systemem • interfejs raportowania i analizy
Moduł raportujący	Moduł raportujący pozwala na: • wyświetlanie zużycia pasma per adres IP i usługę • identyfikowanie niestosownego wykorzystania usług Webowych • dostarczanie szczegółowych raportów na temat ataków • zbieranie i korelowanie błędów sieciowych i systemowych • przedstawianie informacji i zdarzeń związane z tunelami VPN • przedstawianie informacji na temat odwiedzin na stronę firmową/zakładową • zbieranie dziennych logów w celu analizy ruchu.
Obsługiwane platformy	• Windows Server 2012 Standard 64-bit • Windows Server 2012 R2 Standard 64-bit (wersje angielska) • Windows Server 2012 R2 Datacenter • Windows Server 2008 R2 Datacenter • Windows Server 2008 SBS R2 64-bit • Windows Server 2008 R2 Standard 64-bit

	• Windows 8.1 64-bit • Windows 7 64-bit Te wersje Windows mogą być uruchomione jako fizyczne maszyny jak i wirtualne systemy na platformach Hyper-V lub Vmware ESXi (dla Windows Server 2008 i 2012). System wspiera również opcję instalacji jako maszyna wirtualna na platformach: • ESXi 4.1, 5.0, 5.1 i 5.5 • ESXi 4.0 Update 1 (Build 208167 i nowszy) • ESX 4.1 • ESX 4.0 Update 1 (Build 208167 i nowszy)
Dostępne raporty globalne	• Użycie danych • Aplikacje • Aktywność Webowa • Użycie VPN • Zagrożenia • Przeglądanie zdarzeń czasu rzeczywistego (Syslog)
Dostępne raporty per urządzenie	• Użycie danych • Aplikacje • Aktywność Webowa • Aktywność użytkowników • Filtr Webowy • Użycie VPN • Włamania • Botnet • Geo-IP • Wirusy wykryte na Gateway'u • Spyware • Uwierzytelnianie • Raporty kastomizowane • Raport dotyczący analyzera

a)

7. Termin realizacji okablowania sieci LAN

a) Termin realizacji przedmiotu zamówienia do 120 od podpisania umowy.
b) Wykonawca wykonuje Zamawiającemu projekt sieci w dwóch egzemplarzach.
c) Wykonanie projektów uważa się za zakończone jeżeli zostanie on zaakceptowany przez Zamawiającego w terminie 7 dni roboczych od daty złożenia projektów w siedzibie Zamawiającego.
d) Wykonawca przystępuje jednocześnie do prac instalacyjnych nie wcześniej niż po zatwierdzeniu projektów sieci przez Zamawiającego.
e) Wykonawca wykona prace instalacyjne polegające na położeniu sieci elektrycznej i informatycznej, montażu nowych urządzeń aktywnych, szaf dystrybucyjnych, klimatyzacji i przygotowaniu serwerowni w zakresie gotowym do podłączenia urządzeń i sprzętów obecnie znajdujących się w serwerowni tj. serwer, UPS-ów, router-ów.

8. Odbiór i pomiary sieci LAN

Warunkiem koniecznym dla odbioru końcowego instalacji przez Inwestora jest weryfikacja pomiarowa wszystkich zainstalowanych torów transmisyjnych na zgodność parametrów z wymaganiami obowiązujących norm, uzyskanie gwarancji systemowej 30-letniej producenta - wytwórcy okablowania, wykonanie i przekazanie dokumentacji powykonawczych.

1. Wykonawstwo pomiarów powinno być zgodne z normą PN-EN 50346:2004/A1+A2:2009.
2. Pomiary należy wykonać dla wszystkich interfejsów okablowania poziomego oraz szkieletowego.

Należy użyć miernika dynamicznego (analizatora), który posiada oryginalną i najnowszą wersję oprogramowana wewnętrznego (firmware), umożliwiającą dokonanie analizy parametrów, według aktualnie obowiązujących norm. Cały sprzęt pomiarowy musi posiadać aktualną kalibrację i legalizację (tj. certyfikat potwierdzający dokładność jego wskazań, wydany przez serwis producenta).

8.1. Pomiary okablowania miedzianego (sieci LAN)

Pomiary okablowania miedzianego (sieci LAN) należy wykonać:

– miernikiem do pomiarów okablowania miedzianego musi charakteryzować się co najmniej IV klasą dokładności wskazań wg. IEC 61935-1/Ed. 3 (np. Fluke DSX-5000),

– pomiary części miedzianej należy wykonać dla maksymalnej wydajności kablowania, określonej w dokumentacji i skonfrontować z wymaganiami norm ISO/IEC11801:2002/Am2:2010 lub EN50173-1:2011,

– na raporcie (sporządzonym oddzielnie dla każdego pomiaru) mają być widoczne: wynik pomiaru, identyfikacja łącza, wskazanie normy, konfiguracja pomiarowa),

– raport pomiarowy ma jednoznacznie informować o poprawności pomiaru (dobry/zły, pass/fail).

– pomiary należy wykonać w konfiguracji pomiarowej łącza stałego – od gniazda do panela krosowego (ang. „Permanent Link") – przy wykorzystaniu odpowiednich adapterów pomiarowych (z wtykami referencyjnymi) specyfikowanych przez producenta sprzętu pomiarowego.

– pomiar każdego toru transmisyjnego poziomego (miedzianego) powinien zawierać co najmniej:

- mapę połączeń,
- długość połączeń i rezystancje par,
- opóźnienie propagacji oraz różnicę opóźnień propagacji,
- tłumienie,

- NEXT i PS NEXT w dwóch kierunkach,
- ACR-F i PS ACR-F w dwóch kierunkach,
- ACR-N i PS ACR-N w dwóch kierunkach,
- RL w dwóch kierunkach.

8.2. Pomiary okablowania światłowodowego

Pomiary okablowania światłowodowego:

– pomiary sieci światłowodowej mają być wykonane zgodnie z wymaganiami normy PN-EN 14763-3:2009/A1:2010,

– na raporcie (sporządzonym oddzielnie dla każdego łącza) mają być widoczne: wynik pomiaru, identyfikacja łącza, wskazanie normy,

– raport pomiarowy ma jednoznacznie informować o poprawności pomiaru (dobry/zły, pass/fail).

– zalecane jest wykonanie pomiarów włókien światłowodowych za pomocą reflektometru OTDR (np. Fluke OptiFiber Pro lub Fluke DSX-5000 z przystawką OptiFiber) ze względu na pomiar i analizę poszczególnych elementów składowych toru światłowodowego,

– przy pomiarze reflektometrem należy użyć „rozbiegówki" oraz „dobiegówki" w celu określenia jakości wszystkich złączy; wymagane długości dla „rozbiegówki" i „dobiegówki" to minimum 75m dla włókna gradienrowego (MM),

– tłumienie światłowodowego toru transmisyjnego może być wyznaczone za pomocą miernika spadku mocy optycznej lub reflektometru,

– niezależnie od użytego sprzętu pomiarowego kompletny pomiar tłumienia każdego dupleksowego toru transmisyjnego powinien być przeprowadzony w dwie strony w dwóch oknach transmisyjnych:

- od punktu A do punktu B w oknie 850nm i 1300nm,
- od punktu B do punktu A w oknie 850nm i 1300nm.

8.3. Dokumentacja powykonawcza

Dokumentacja powykonawcza ma zawierać:
- raporty z pomiarów dynamicznych okablowania,
- rzeczywiste trasy prowadzenia kabli transmisyjnych poziomych,
- oznaczenia poszczególnych szaf, gniazd, kabli i portów w panelach krosowych,
- lokalizację przebić przez ściany i podłogi,
- raporty pomiarowe wszystkich torów transmisyjnych należy zawrzeć w dokumentacji powykonawczej i przekazać inwestorowi przy odbiorze inwestycji.

9. Gwarancja

Należy zapewnić objęcie wykonanej instalacji gwarancją systemową producenta, gdzie okres gwarancji udzielony przez producenta nie może być krótszy niż 30 lat (zamawiający wymaga certyfikatu producenta okablowania udzielonego bezpośrednio użytkownikowi końcowemu i stanowiącego 30-letnie zobowiązanie gwarancyjne producenta wszystkich elementów całego systemu okablowania dotrzymania parametrów jakościowych i materiałowych).
Okres gwarancji ma być standardowo udzielany przez producenta okablowania, tzn. na warunkach oficjalnych, ogólnie znanych, dostępnych i opublikowanych. Tym samym oświadczenia o specjalnie wydłużonych okresach gwarancji wystawione przez producentów, dostawców, dystrybutorów, pośredników, wykonawców lub innych nie będą uznawane za wiarygodne i spowodują bezwzględne odrzucenie oferty.
Okres gwarancji liczony jest od dnia, w którym podpisano protokół końcowego odbioru prac i producent okablowania wystawił certyfikat gwarancyjny.

10. Dodatkowe warunki budowy okablowania strukturalnego

Zadanie opisane powyżej może być realizowane w godzinach 7.30 do 17.30. od poniedziałku do piątku (administracja tylko do 14:30).

Wszystkie materiały wprowadzone do robót winny być nowe, nieużywane, najnowszych aktualnych wzorów, winny również uwzględniać wszystkie nowoczesne rozwiązania techniczne.

11. Adaptacja pomieszczenia Serwerowni

Pomieszczenie techniczne serwerowni to centrum danych, dlatego też pomieszczenie Serwerowni musi spełniać szczególne warunki związane z bezpieczeństwem oraz dostępem do niego osób niepowołanych.

Opisane poniżej prace oraz parametry planowanych urządzeń należy taktować jako minimalne. Urządzenia i osprzęt wyspecyfikowany w zestawieniu materiałów należy traktować jako przykładowy i może zostać zamieniony na inny pod warunkiem, że dostawca przedstawi dokumenty, że aparatura zamienna ma te same lub lepsze parametry techniczne od zaproponowanej, taką sama barwę i okres gwarancji.

11.1. Założenia do przebudowy pomieszczenia na serwerownię

Stan techniczny budynku

Budynek, w którym zaplanowano pomieszczenie Podstawowej Serwerowni to nowowybudowany budynek Izby Przyjęć. Zaplanowano wykorzystanie pomieszczenia nr 1.09 znajdującego się w Piwnicach budynku.
Budynek i jego elementy konstrukcyjne są w bardzo dobrym stanie technicznym i mają odpowiednią nośność dla przewidywanej funkcji.
W adaptowanych pomieszczeniach nie będzie prac budowlanych ingerujących w konstrukcje nośne istniejącego budynku.

Budynek, w którym zaplanowano pomieszczenie drugiej Serwerowni to budynek Administracji. Zaplanowano wykorzystanie pomieszczenia nr 114 znajdującego się na 1 piętrze budynku.
Budynek i jego elementy konstrukcyjne są w dobrym stanie technicznym i mają odpowiednią nośność dla przewidywanej funkcji.
W adaptowanych pomieszczeniach nie będzie prac budowlanych ingerujących w konstrukcje nośne istniejącego budynku.

Zakres prac

Wydziela się pod względem pożarowym pomieszczenie Podstawowej Serwerowni z uwagi na wymogi w tym zakresie. Planuje się również wymianę drzwi w pomieszczeniu Podstawowej jak i drugiej serwerowni na posiadające odporność ogniową klasy EI 30. Projektowana jest wewnętrzna linia zasilająca elektryczna wydzielona dla potrzeb obu Serwerowni.

Wykonać/zaplanować niezbędne Instalacje :

- klimatyzacja - klimatyzacja pomieszczenia

Pomieszczenie serwerowni musi być klimatyzowane ze względu na dużą koncentrację urządzeń pracujących w sposób ciągły i wydzielających duże ilości ciepła.

Wydajność klimatyzacji powinna być dostosowana do podanej przez producentów sprzętu emisji ciepła. Należy przewidzieć pracę redundantną min. dwóch niezależnych klimatyzatorów.

- elektryczna i gniazd wtykowych

Doprowadzenie zasilania GPD z uwzględnieniem zapasu mocy.
Instalacja gniazd wtykowych dedykowanych dla potrzeb szaf i wszystkich dodatkowych systemów instalowanych w Serwerowni.

- techniczna /logiczna

Doprowadzenia światłowodów oraz okablowania logicznego w odpowiedniej ilości.

- kontroli dostępu, CCTV, SSWiN

KD - System kontroli dostępu obejmować powinno drzwi do pomieszczenia serwerowni GPD oraz wejścia do pomieszczeń biurowych informatyków.

CCTV - System monitoringu wizyjnego (CCTV) obejmować będzie pomieszczenie serwerowni.
Zalecamy rozwiązanie oparte o sieciowy rejestrator i kamery cyfrowe IP
Materiał video powinien być przetrzymywany przez 30 dni.

SSWIN - System alarmowy obejmować powinien obejmować pomieszczenie serwerowni GPD oraz pomieszczenia biurowe informatyków.

Roboty rozbiórkowe – dotyczy obu Serwerowni:

- demontaż drzwi w pomieszczeniu podstawowej oraz drugiej serwerowni,
- wykonanie otworu drzwiowego,
- uszczelnienie pomieszczenia,
- wykonanie przekuć do przejść instalacyjnych.

Roboty budowlane – dotyczy obu Serwerowni:

- obrobienie istniejących otworów drzwiowych,
- montaż drzwi p.poż. pełnych,
- montaż instalacji elektrycznych, LAN.

Założenia funkcjonalne

W pomieszczeniach obu Serwerowni zamontowane będą urządzenia do obsługi systemu komputerowego. W pomieszczeniu nie będzie przebywać obsługa - będzie jedynie dozorowane.
W pomieszczeniach zainstalowane będą również urządzenia monitorujące prace serwerowni.

Projektowane roboty budowlane

Montaż drzwi wejściowych do pomieszczeń przeznczonych na serwerownię – o klasie odporności ogniowej EI30.

Instalacje – podstawowa serwerownia:

- klimatyzacja - klimatyzacja pomieszczenia - wg cz. Instalacyjnej,
- elektryczna i gniazd wtykowych - wg cz. elektrycznej,
- techniczna /logiczna - wg cz. technicznej,
- kontroli dostępu, SSWiN - wg cz. technicznej,
- gaszenia gazem – wg cz. gaszenie gazem.

Instalacje – druga serwerownia:

- klimatyzacja - klimatyzacja pomieszczenia – zaplanowano wykorzystanie istniejący klimatyzatora HITACHI,
- elektryczna i gniazd wtykowych - wg cz. elektrycznej,
- techniczna /logiczna - wg cz. technicznej,
- kontroli dostępu, SSWiN - wg cz. technicznej,
- gaszenia gazem – wg cz. gaszenie gazem.

Uwaga: przejścia instalacyjne i ich budowy wykonać w klasie odporności ogniowej odpowiedniej do wymogów dla danej przegrody (dotyczy przejść i instalacji o średnicy otworu większego od 4 cm).

11.2. System sygnalizacji włamania i napadu oraz kontroli dostępu

System alarmowy oraz kontroli dostępu obejmować będzie pomieszczenie serwerowni SRV oraz pomieszczenie drugiej serwerowni GPD. Będą to dwa niezależne systemy.
Zaprojektowano rozwiązanie oparte o centralę alarmową zintegrowaną z systemem kontroli dostępu. Dzięki szerokiej gamie modułów rozszerzeń, ich możliwości mogą być dostosowane do bieżących potrzeb. Dużym atutem zaprojektowanych central są ich możliwości komunikacyjne w połączeniu z dodatkowymi modułami – GSM oraz TCP/IP.

System SSWiN wraz z KD składał się będzie z następujących podzespołów (1 zestaw):

- Centrala systemu alarmowego, do 32 wejść i wyjść
- Klawiatura obsługi systemu alarmowego LCD z czytnikiem zbliżeniowym, biała podświetleniem
- Moduł rozbudowy czytników kart/pastylek centrali systemu alarmowego
- Ethernetowy moduł komunikacyjny
- Przycisk awaryjnego wyjścia, zielony, podwójny, klapka zabezpieczająca
- Zwora 270kg z przekaźnikiem wraz z elementem mocowania

- Moduł rozbudowy centrali systemu alarmowego, komunikacyjny, monitoring GPRS/SMS wraz z Anteną 900/1800MHz
- Sygnalizator optyczno-akustyczny, wewnętrzny, czerwony
- Sygnalizator optyczno-akustyczny, zewnętrzny, z czerwonym światłem stroboskopowym
- Obudowa central natynkowa
- Akumulator 12V, 18Ah
- Czujka ruchu dualna PIR+MW, wewnętrzna
- Czujka zalania wody
- Czujka pożarowa systemu alarmowego, optyczno-temperaturowa
- Programowalna czujka temperatury
- Karta ISO UNIQUE – 10 sztuk

Parametry techniczne płyty głównej:

- obsługa od 8 do 32 wejść
- możliwość podziału systemu na 16 stref, 4 partycje
- obsługa od 8 do 32 programowalnych wyjść
- magistrale komunikacyjne do podłączania manipulatorów i modułów rozszerzeń
- wbudowany komunikator telefoniczny z funkcją monitoringu, powiadamiania głosowego i zdalnego sterowania
- obsługa systemu przy pomocy manipulatorów LCD, klawiatur strefowych, pilotów i kart zbliżeniowych oraz zdalnie z użyciem komputera lub telefonu komórkowego
- 28 niezależnych timerów do automatycznego sterowania
- funkcje kontroli dostępu i automatyki domowej
- pamięć min. 400 zdarzeń z funkcją wydruku
- obsługa do 64+4+1 użytkowników
- port RS-232 - gniazdo RJ
- możliwość aktualizacji oprogramowania za pomocą komputera
- wbudowany zasilacz impulsowy o wydajności 1,2 A z funkcjami ładowania akumulatora i diagnostyki

Parametry techniczne manipulatora z wbudowanym czytnikiem kart zbliżeniowych:

- podświetlenie klawiatury i wyświetlacza
- diody LED informujące o stanie systemu
- alarmy NAPAD, POŻAR, POMOC wywoływane z klawiatury
- sygnalizacja dźwiękowa wybranych zdarzeń w systemie
- wbudowany czytnik kart zbliżeniowych do obsługi systemu

Parametry techniczne modułu rozbudowy czytników kart/pastylek:

- kompatybilność z czytnikami wykorzystującymi format Wiegand 26
- przekaźnik do sterowania elektrozworą/ryglem elektrycznym
- wejście do kontroli stanu drzwi
- wejście umożliwiające otwieranie przejścia przy pomocy przycisku
- funkcja odblokowania drzwi przy alarmie pożarowym
- wejście przeciwsabotażowe

Parametry techniczne Ethernetowego modułu komunikacyjnego:

- współpraca z projektowanymi centralami alarmowymi
- monitoring TCP/IP lub UDP
- programowanie za pomocą dedykowanego oprogramowania
- nadzór systemu
- obsługa systemu z poziomu przeglądarki WWW
- obsługa systemu z telefonu komórkowego za pomocą dedykowanej aplikacji
- kodowanie transmisji danych
- obsługa automatycznej konfiguracji adresów DHCP

Parametry techniczne modułu monitoringu GPRS/SMS:

- moduł wykorzystuje przemysłowy telefon GSM i wymaga karty SIM z odpowiednio dobranym planem taryfowym lub prepaid, umożliwiającej korzystanie z technologii GPRS. W przypadku kart przedpłaconych moduł daje także możliwość skontrolowania salda dostępnych środków oraz ważności konta.
- 5 wejść wyzwalających monitoring lub powiadamianie
- automatyczne przełączenie na SMS w przypadku braku GPRS
- powiadamianie SMS/CLIP
- zdalne sterowanie wyjściem modułu
- wysyłanie transmisji testowej z wykorzystaniem CLIP
- sygnalizacja awarii łączności

Parametry techniczne sygnalizatora wewnętrznego:

- Typ produktu Sygnalizator akustyczno-optyczny wewn.
- Kolor klosza Czerwony
- Kolor obudowy Biały
- Źródło dźwięku Przetwornik piezoelektryczny
- Natężenie dźwięku (dB) 110

Parametry techniczne sygnalizatora zewnętrznego:

- Typ produktu Sygnalizator optyczno-akustyczny zewn.
- Zabezpieczenie oderwania od podłoża Tak

- Zabezpieczenie przed ingerencją w produkt Tak
- Kolor klosza Czerwony
- Kolor obudowy Biały
- Źródło dźwięku Przetwornik piezoelektryczny
- Natężenie dźwięku (dB) 120

Parametry techniczne mikroprocesorowej czujki dualnej (PIR+MW):

- Typ produktu Czujka dualna PIR+MW
- Zasięg (m) 15
- Kąt widzenia (st) 90°
- Rodzaj optyki Fresnela
- Analiza sygnału Cyfrowa
- Stopień zabezpieczenia Grade 2
- Pamięć alarmu Tak
- Wysokość montażu 1,5...3,1 m
- Kompensacja temperatury Cyfrowa
- Kolor Biały

Parametry techniczne cyfrowej czujki optyczno-termicznej:

- Typ produktu Czujka pożarowa
- Autotest Tak
- Zasięg (m) 3,5
- Detekcja dymu Tak
- Detekcja temperatury Tak
- Analiza sygnału Cyfrowa
- Sygnalizacja alarmu Tak
- Pamięć alarmu Tak
- Resetowanie Tak
- Wyjście NC
- Temperatura pracy (°C) -10...+55

Parametry techniczne programowalnego czujka temperatury:

- programowanie progów i gradientu temperatury
- możliwość pracy w dwóch trybach (funkcja oszczędności)
- możliwość podłączenia zewnętrznej sondy temperatury
- dwa wyjścia przekaźnikowe do sterowania urządzeniami zewnętrznymi

Parametry techniczne karty zbliżeniowej:

- Typ produktu ISO Unique 125kHz z nadrukowanym numerem
- Częstotliwość 125kHz

- Akcesoria etui miękkie
- Zasięg odczytu (m) 0,1

11.3. System monitoringu wizyjnego w Serwerowniach

System monitoringu CCTV obejmować będzie pomieszczenie serwerowni SRV (dwie kamery) oraz pomieszczenie drugiej serwerowni GPD (dwie kamery).
Zaprojektowano rozwiązanie oparte o rejestratory i kamery IP. System będzie składał się z 4 kamer oraz dwóch rejestratorów. Zainstalowane zostaną one: 2 kamery i rejestrator w pomieszczeniu SVR oraz 2 kamery i rejestrator w pomieszczeniu GPD. Oba rejestratory będą zapisywać obraz ze wszystkich kamer, dzięki takiemu rozwiązaniu uzyskana zostanie redundancja zapisu obrazu z kamer na wypadek awarii jednego z rejestratorów.

Parametry techniczne rejestratorów:

- Typ rejestratora rejestrator IP z możliwością obsługi do 8 kamer
- Pasmo wejściowe min. 80Mb/s
- Pasmo wyjściowe min. 80Mb/s
- Obsługa kompresji wideo min.: H.264, H264+
- Obsługa rozdzielczości 6 MP / 5MP / 3MP / 1080p / UXGA / 720p / VGA / 4CIF
- Interfejs sieciowy 1 x RJ45, 1Gb/s (1000BASE-T)
- Interfejsy USB 1 x USB 2.0, 1 x USB 3.0
- Interfejsy kamer 8 x 100 Mb/s PoE+ (802.3at)
- Moc PoE min. 100 W
- Obsługa dysków min. 2 x HDD 3,5'' SATA
- Zainstalowane dyski 2 x HDD SATA min. 4TB (dysk dedykowany do pracy w systemach monitoringu)
- Obudowa 1U, 19'' (montaż w szafie rack)
- Zasilanie 230 VAC

Parametry techniczne kamer:

- Typ kamery kamera IP kopułowa zewnętrzna
- Przetwornik obrazu min. 1/2.8'' CMOS 4Mpix
- Rozdzielczość (px) min. 4Mpix (2688 × 1520)
- Kompresja wideo min.: H.264, MJPEG, H264+
- Ilość strumieni wideo min. 2
- Funkcja dzień / noc mechaniczny filtr podczerwieni
- Ilość klatek min.: 20fps (2688x1520), 25fps (1920x1080)
- Obiektyw f=2.8mm /F2.0
- Zakres dynamiki min. 120dB

- Funkcje kamery trueWDR, BLC, 3DNR
- Promiennik podczerwieni IR zasięg do 30m
- Zgodność ze standardami ONVIF (PROFILE S, PROFILE G), PSIA, CGI, ISAPI
- Obsługa kart pamięci SD/SDHC/SDXC, do min. 128GB
- IP obudowy min. IP66
- IK obudowy min. IK10
- Zasilanie 12 VDC / PoE
- Pobór mocy max. 6W

11.4. Instalacja elektryczna

Dla potrzeb zasilania Serwerowni wykonane zostanie nowe zasilanie z rozdzielni głównej budynku Izby Przyjęć, dedykowana rozdzielnia elektryczna dla potrzeb serwerowni została uwzględniona w części instalacji elektrycznych.

Dla zasilania Serwerowni Podstawowej należy zaprojektować i wykonać dedykowaną rozdzielnię elektryczną zasilaną z rozdzielni głównej Budynku Izby Przyjęć.

Dedykowana rozdzielnia elektryczna w Serwerowni będzie zasilać:

- szafa serwerowa – trzy dedykowane obwody,
- urządzenia SSWiN oraz KD – jeden dedykowany obwód,
- urządzenia klimatyzacji – dwa dedykowane obwody.

Instalację elektryczną należy wykonać zgodnie z należy wykonać zgodnie z obowiązującymi przepisami szczegółowymi dla tego typu działania oraz przepisami wykonawczymi SEP i norm Prawa Budowlanego.

11.5. Klimatyzacja

Pomieszczenie serwerowni musi być klimatyzowane ze względu na dużą koncentrację urządzeń pracujących w sposób ciągły i wydzielających duże ilości ciepła. Wydajność klimatyzacji powinna być dostosowana do podanej przez producentów sprzętu emisji ciepła. Należy przewidzieć pracę redundantną min. dwóch niezależnych klimatyzatorów.

Zaprojektowano system chłodzenia opary na dwóch jednostkach, z których każda zapewnia 70% pokrycie zapotrzebowanie chłodzenia pomieszczenia przy maksymalnym obciążeniu zainstalowanych urządzeń.

Zaprojektowano dwa klimatyzatory pracujące naprzemiennie o mocy chłodniczej 5,2kW wraz ze sterownikiem pracy naprzemiennej oraz dwie pompki do skroplin.

Funkcje klimatyzatora:

- Nowoczesna technologia DC Inverter
- Filtr polifenolowy
- Tryb pracy: auto, chłodzenie, grzanie, osuszanie, wentylacja

- Unikalna funkcja osuszania wnętrza
- Automatyczne ustawianie żaluzji
- Filtr jonowy o wydłużonej żywotności
- Elektrostatyczny filtr antybakteryjny
- Energooszczędność w trybie chłodzenia i grzania - klasa energetyczna A
- Innowacyjna konstrukcja wymiennika
- Programator czasowy: włącz/wyłącz
- Auto restart
- Ergonomiczny bezprzewodowy pilot
- Tryb pracy nocnej (Quiet)
- Regulacja siły nawiewu z pilota
- 24-godzinne programowanie
- Atesty - PZH

Dane techniczne klimatyzatorów:
Zasilanie (V/Ø/Hz) 230/1/50
Wydajność chłodzenia (kW) min. 5.00
Wydajność grzania (kW) min. 6.00
Klasa energetyczna A/A
Zakres pracy (chłodzenie) -10 ~ +43
Zakres pracy (grzanie) -15 ~ +24
Czynnik chłodniczy R410A

11.6. Wymiana drzwi

Pomieszczenie Serwerowni powinno być zabezpieczone przed dostępem osób niepowołanych. W tym celu zamontowane zostaną drzwi wejściowe do pomieszczeń obu Serwerowni. Istniejące drzwi do pomieszczeń zostaną zdemontowane wraz z ościeżnicą.
Proponujemy drzwi atestowane przeciwpożarowe, o wymiarach 90x200.
Dane techniczne:
- zamek główny składający się z zamka centralnego, pomocniczego oraz rygla pionowego,
- zawiasy trójdzielne,
- tłumienie akustyczne 45 dB,
- przeciwpożarowe – odporność ogniowa EI-30,
- dymoszczelność Sa, Sm,
- antywłamaniowe klasy C,
- samozamykacz.

11.7. Przenośne Urządzenie Gaśnicze

Pomieszczenie Serwerowni zostanie wyposażone w przenośne Urządzenia Gaśnicze – czyli specjalne gaśnice przeznaczone do gaszenia pożarów z grupy B i C pod napięciem. Gaśnica takiego typu zalecana jest wszędzie tam gdzie wymagana jest wysoka skuteczność oraz brak zanieczyszczeń po środku gaśniczym.
Dedykowana jest do:
- do gaszenia czułych urządzeń elektronicznych i elektrycznych,
- w serwerowniach, w archiwach, w muzeach,
- w laboratoriach, jak również w pomieszczeniach biurowych.

Podstawowe cechy
- gaśnica na gaz FE-36 będący czystym środkiem gaśniczym
- niezwykle skuteczne i w pełni bezpieczne rozwiązanie wśród nowoczesnych, podręcznych sprzętów gaśniczych
- Świadectwo Dopuszczenia wydane przez Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej w Józefowie
- możliwość wielokrotnego napełniania w Autoryzowanych Zakładach Serwisowych
- niewielkie gabaryty, poręczna budowa sprzyjają swobodnemu użytkowaniu przez każdą, nawet nieprzeszkoloną osobę
- wieszak w komplecie
- masa środka gaśniczego 2 kg

Zaplanowano dostarczenie po dwie gaśnice na każdą Serwerownię.

12. Sprzęt serwerowy

Wymagania ogólne dotyczące sprzętu serwerowego

a) Wszystkie oferowane urządzenia muszą być wyprodukowane zgodnie z normą jakości ISO 9001:2008 lub normą równoważną.
b) W momencie oferowana wszystkie elementy oferowanej architektury muszą być dostępne (dostarczane) przez producenta.
c) Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
d) Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych.
e) Do każdego dostarczonego wraz z serwerem systemu operacyjnego muszą być załączone oryginalne dokumenty licencyjne uprawniające do używania systemu operacyjnego określonego dla każdego z serwerów
f) Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej.
g) Wszystkie serwery muszą posiadać Certyfikat CE produktu albo spełniać normy równoważne.
h) Oferowane serwery muszą być przygotowane do współpracy z systemami operacyjnymi takimi jak: Microsoft Windows Server 2012 R2, Microsoft Windows Server 2012, LINUX Red Hat, VMware
i) Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach : 230 V ± 10% , 50 Hz.
j) Sprzęt powinien być objęty gwarancją producenta sprzętu przez okres min. 3 lat.
k) Wszystkie poniższe parametry należy traktować jako minimalne.
l) Wszelkie użyte nazwy własne producentów należy traktować informacyjnie i dopuszczona jest możliwość zastosowania technologii w inny sposób zapewniających poniższe funkcjonalności.

Zaprojektowano serwery produkcyjne w popularnym rozmiarze 2S/2U, które można z łatwością skonfigurować jako niezawodny serwer ogólnego przeznaczenia do zastosowań o kluczowym znaczeniu biznesowym, oferujący skalowalną pamięć masową, automatyczne zarządzanie oraz funkcje wysokiej dostępności, takie jak:

- Zasilacze nadmiarowe (PSU)
- Dyski twarde i zasilacze nadmiarowe z możliwością wymiany bez wyłączania systemu
- Obsługa dwóch kart SD na potrzeby awaryjnego przełączania monitorów maszyn wirtualnych
- Inteligentne funkcje wbudowane w zintegrowany kontroler

- Usługa pomocy technicznej, która zapewnia, bezpośredni dostęp przez telefon i online do wykwalifikowanych techników w danym regionie.

Usługa Zachowaj swój dysk twardy pozwala klientom zachować uszkodzone dyski twarde po otrzymaniu dysku twardego objętego programem Kwalifikowanej naprawy. „Kwalifikowana naprawa" obejmuje naprawę wad wykonania i/lub wymianę sprzętu podlegającego gwarancji na sprzęt dotyczącej Produktu objętego pomocą techniczną.

12.1. Serwery produkcyjne – 2szt.

Zaprojektowano użycie dwóch serwerów jako serwerów produkcyjne (aplikacyjny i bazodanowy), które z wykorzystaniem wirtualizatora będą uruchamiały maszyny wirtualne potrzebne do obsługi informatycznej Szpitala. Serwery te będą pracowały z wykorzystaniem funkcji klastra.

Każdy z serwerów (aplikacyjny i bazodanowy) powinien mieć następującą konfigurację:

- Obudowa o wysokości maksymalnie 2 U z zestawem umożliwiającym montaż w szafie rack 19"
- Dwa procesory min. 10 rdzeniowe, taktowany zegarem min 2.2 GHz.
- Pamięć RAM min. 128GB typu Registered
- Płyta główna dedykowana do pracy w serwerach
- Zainstalowane dwa dyski twarde 300GB SAS 15k
- Zainstalowane dwie karty SD o pojemności 16Gb każda na wirtualizator
- Kontroler macierzowy umożliwiający konfigurację dysków w RAID 0/1/10/5/6 z podtrzymaniem pamięci kontrolera typu flash
- Karta sieciowa z 4 portami Gbit Ethernet zakończone złączem RJ-45
- Karta sieciowa dodatkowa z 2 portami 10 Gbit Ethernet zakończona złączem SFP+
- Dwie karty jednoportowe Fibre Channel 16 GB
- Karta graficzna zintegrowana na płycie głównej
- Dwa zasilacze reduntantne, typu Hot-Plug
- Wentylatory reduntantne, typu Hot-Plug
- Zarządzanie - Serwer wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty zdalnego zarządzania, przejęcie pełnej konsoli serwera niezależnie od jego stanu (także podczas startu, restartu OS).

Specyfikacja istotnych warunków zamówienia dla serwera:

Nazwa komponentu	***Wymagane minimalne parametry techniczne***
Obudowa	Obudowa typu Rack o wysokości maksymalnej 2U, wraz kompletem szyn umożliwiających montaż w standardowej szafie Rack, wysuwanie serwera do celów serwisowych wraz z organizatorem kabli.
Płyta główna	Z możliwością instalacji minimum dwóch fizycznych procesorów, posiadająca minimum 12 slotów na pamięci z możliwością zainstalowania do minimum 384GB 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	Dwa procesory min. ośmiordzeniowe dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku minimum 660 punktów w teście SPECint_rate_base2006 dostępnym na stronie internetowej www.spec.org dla konfiguracji dwuprocesorowej Do oferty należy załączyć wynik testu dla oferowanego modelu serwera wraz z oferowanym modelem procesora.
RAM	Minimum 128 GB pamięci RAM o częstotliwości taktowania minimum 2133MHz
Sloty PCI Express	Minimum 3 sloty PCI Express
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, min. 1x VGA D-Sub
Karta graficzna	Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1280x1024 pikseli
Interfejsy sieciowe	Minimum cztery interfejsy sieciowe 1Gb/s Ethernet ze złączami BaseT nie zajmujące żadnego z dostępnych slotów PCI Express oraz złącz USB. Karta sieciowa dodatkowa z 2 portami 10 Gbit Ethernet zakończona złączem SFP+ wraz z kablem SFP+ to SFP+ 10GbE do połączeń bezpośrednich o długości 3m. Dwie karty jednoportowe Fibre Channel 16 GB.
Kontroler pamięci masowej	Sprzętowy kontroler dyskowy, umożliwiający obsługę dysków z prędkościami transferu 3, 6, 12 Gb/s; umożliwiający skonfigurowanie na wewnętrznej pamięci dyskowej zabezpieczeń RAID: 0, 1, 5, 6, 10, 50, 60, wyposażony w wbudowaną, nieulotną pamięć cache o pojemności min. 1GB.
Wewnętrzna pamięć masowa	Możliwość instalacji min. 48TB w wewnętrznej pamięci masowej typu Hot Plug 7.2k RPM, możliwość instalacji dysków twardych typu: SATA, NearLine SAS, SAS, SSD, PCI Express Flash oraz SED dostępnych w ofercie producenta serwera. Zainstalowane 2 dyski twarde o poj. min. 300GB SAS 15k RPM każdy skonfigurowane fabrycznie w RAID 1.

Napęd optyczny	Zainstalowany wewnętrzny napęd umożliwiający odczyt i zapis nośników DVD
System operacyjny	Wykonawca dostarczy 2 licencje na serwerowy system operacyjny SSO opisany w dalszej części dokumentu.
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. – 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	Minimum 4 redundantne wentylatory pracujące w trybie Fault Tolerant. Dwa redundantne zasilacze Hot Plug o mocy minimum 690 Wat każdy wraz z kablami zasilającymi.
Karta zarządzająca	Niezależna od zainstalowanego systemu operacyjnego, zintegrowana z płytą główną posiadająca port RJ45 lub jako dodatkowa karta rozszerzeń (Zamawiający dopuszcza zastosowanie karty instalowanej w slocie PCI Express jednak nie może ona powodować zmniejszenia minimalnej ilości wymaganych slotów w serwerze), posiadająca minimalną funkcjonalność: - 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 - 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 Możliwość rozbudowy funkcjonalności karty o automatyczne przywracanie ustawień serwera, kart sieciowych, BIOS, wersji firmware w przypadku awarii i wymiany któregoś z komponentów dedykowanej pamięci flash(w tym kontrolera RAID, kart sieciowych, płyty głównej).

Warunki gwarancji dla serwera	3 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. W przypadku awarii, dyski twarde pozostają własnością Zamawiającego. Do oferty należy załączyć oświadczenie potwierdzające o spełnieniu tego warunku. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. Możliwość telefonicznego i elektronicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta oraz poprzez stronę internetową producenta lub jego przedstawiciela. Dokumentacja dostarczona wraz z serwerem dostępna w języku polskim lub angielskim. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie najnowszych uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001 Serwer musi posiadać deklaracja CE (dokument załączyć do oferty) Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2008 R2 x64, Microsoft Windows Server 2012 oraz Microsoft Server 2012 R2 Zgodność z systemami SUSE Linux Enterprise Server, RedHat Enterprise Linux, Citrix XenServer, VMware vSphere.

12.2. Serwer backupowy – 1szt.

Do obsługi systemu backupu zaprojektowano serwer 2U/2S, zlokalizowany w drugiej Serwerowni w budynku ADM.

Zaprojektowano użycie serwera DELL R530 jako serwer kopii zapasowych, który z wykorzystaniem oprogramowania backupowego będzie wykonywał kopie zapasowe maszyn wirtualnych zainstalowanych na maszynach produkcyjnych.

Serwer backupowy powinien mieć następującą konfigurację:

- Obudowa o wysokości maksymalnie 2 U z zestawem umożliwiającym montaż w szafie rack 19”
- Jeden procesor min. 8 rdzeniowy, taktowany zegarem min 2.2 GHz z możliwością zainstalowania drugiego procesora
- Pamięć RAM min. 64GB typu Registered
- Płyta główna dedykowana do pracy w serwerach
- Zainstalowane dwa dyski twarde 300GB SAS 15k oraz trzy dyski twarde 4TB NLSAS
- Zainstalowane dwie karty SD o pojemności 16Gb każda na wirtualizator
- Kontroler macierzowy umożliwiający konfigurację dysków w RAID 0/1/10/5/6 z podtrzymaniem pamięci kontrolera typu flash
- Karta sieciowa z 4 portami Gbit Ethernet zakończone złączem RJ-45
- Karta SAS HBA do podłączenia biblioteki taśmowej
- Dwie karty jednoportowe Fibre Channel 16 GB
- Karta graficzna zintegrowana na płycie głównej
- Dwa zasilacze reduntantne, typu Hot-Plug
- Wentylatory reduntantne, typu Hot-Plug
- Zarządzanie - Serwer wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty zdalnego zarządzania, przejęcie pełnej konsoli serwera niezależnie od jego stanu (także podczas startu, restartu OS).

Specyfikacja dla serwera:
Serwer backupowy

Nazwa komponentu	***Wymagane minimalne parametry techniczne***
Obudowa	Obudowa typu Rack o wysokości maksymalnej 2U, wraz kompletem szyn umożliwiających montaż w standardowej szafie Rack, wysuwanie serwera do celów serwisowych wraz z organizatorem kabli.
Płyta główna	Z możliwością instalacji minimum dwóch fizycznych procesorów, posiadająca minimum 12 slotów na pamięci z możliwością zainstalowania do minimum 384GB 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	Jeden procesor min. ośmiordzeniowy dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku minimum 629 punktów w teście SPECint_rate_base2006 dostępnym na stronie internetowej www.spec.org dla konfiguracji

	dwuprocesorowej. Do oferty należy załączyć wynik testu dla oferowanego modelu serwera wraz z oferowanym modelem procesora.
RAM	Minimum 64 GB pamięci RAM o częstotliwości taktowania minimum 2133MHz
Sloty PCI Express	Minimum 3 sloty PCI Express
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, min. 1x VGA D-Sub
Karta graficzna	Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1280x1024 pikseli
Interfejsy sieciowe	Minimum cztery interfejsy sieciowe 1Gb/s Ethernet ze złączami BaseT nie zajmujące żadnego z dostępnych slotów PCI Express oraz złącz USB. Karta SAS HBA do podłączenia biblioteki taśmowej Dwie karty jednoportowe Fibre Channel 16 GB
Kontroler pamięci masowej	Sprzętowy kontroler dyskowy, umożliwiający obsługę dysków z prędkościami transferu 3, 6, 12 Gb/s; umożliwiający skonfigurowanie na wewnętrznej pamięci dyskowej zabezpieczeń RAID: 0, 1, 5, 6, 10, 50, 60, wyposażony w wbudowaną, nieulotną pamięć cache o pojemności min. 1GB.
Wewnętrzna pamięć masowa	Możliwość instalacji min. 48TB w wewnętrznej pamięci masowej typu Hot Plug 7.2k RPM, możliwość instalacji dysków twardych typu: SATA, NearLine SAS, SAS, SSD, PCI Express Flash oraz SED dostępnych w ofercie producenta serwera. Zainstalowane 2 dyski twarde o poj. min. 300GB SAS 15k RPM każdy skonfigurowane fabrycznie w RAID 1 Zainstalowane 3 dyski twarde o poj. min. 4TB NLSAS 7,2k RPM każdy skonfigurowane fabrycznie w RAID 5
Napęd optyczny	Zainstalowany wewnętrzny napęd umożliwiający odczyt i zapis nośników DVD
System operacyjny	Wykonawca dostarczy 1 licencję na serwerowy system operacyjny SSO opisany w dalszej części dokumentu.
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. – 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	Minimum 4 redundantne wentylatory pracujące w trybie Fault Tolerant.

	Dwa redundantne zasilacze Hot Plug o mocy minimum 650 Wat każdy wraz z kablami zasilającymi.
Karta zarządzająca	Niezależna od zainstalowanego systemu operacyjnego, zintegrowana z płytą główną posiadająca port RJ45 lub jako dodatkowa karta rozszerzeń (Zamawiający dopuszcza zastosowanie karty instalowanej w slocie PCI Express jednak nie może ona powodować zmniejszenia minimalnej ilości wymaganych slotów w serwerze), posiadająca minimalną funkcjonalność: - 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 - 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 Możliwość rozbudowy funkcjonalności karty o automatyczne przywracanie ustawień serwera, kart sieciowych, BIOS, wersji firmware w przypadku awarii i wymiany któregoś z komponentów dedykowanej pamięci flash (w tym kontrolera RAID, kart sieciowych, płyty głównej).
Warunki gwarancji dla serwera	3 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. W przypadku awarii, dyski twarde pozostają własnością Zamawiającego. Do oferty należy załączyć oświadczenie potwierdzające o spełnieniu tego warunku. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. Możliwość telefonicznego i elektronicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta oraz poprzez stronę internetową producenta lub jego przedstawiciela. Dokumentacja dostarczona wraz z serwerem dostępna w języku polskim lub angielskim. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie

	najnowszych uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001 Serwer musi posiadać deklaracja CE (dokument załączyć do oferty) Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2008 R2 x64, Microsoft Windows Server 2012 oraz Microsoft Server 2012 R2 Zgodność z systemami SUSE Linux Enterprise Server, RedHat Enterprise Linux, Citrix XenServer, VMware vSphere.

12.3. System macierzy dyskowej

System pamięci masowej zaprojektowano w oparciu o urządzenie z serii macierzy Fibre Channel. Macierze te są idealne do konsolidacji pamięci masowej klasy podstawowej, która wymaga wysokiej dostępności, wysokiej wydajności, ciągłości działania oraz niezawodności.

Cechy wspólne

- Intuicyjne, zaawansowane oprogramowanie do zarządzania pamięcią masową.
- Obsługa interfejsów 16 Gb FC umożliwiająca budowę konfiguracji SAN zawierających pamięci o różnej szybkości.
- Możliwość tworzenia kombinacji napędów i obudów rozszerzeń pozwala na dopasowanie systemu do większości zastosowań, przy jednoczesnym ograniczeniu zużycia energii i miejsca.
- Skalowalność do 192 napędów. System jest przystosowany do elastycznej rozbudowy w miarę przyrostu wolumenu danych i pojawiania się nowych potrzeb. Rozbudowa poprzez złącza 12Gb SAS.
- Obsługa napędów SAS (NL). Napędy dysków SAS (NL — nearline) są często oczywistą alternatywą dla napędów SATA. Napędy SAS NL, dostępne w cenach porównywalnych z cenami napędów SATA, oferują znacznie większą wydajność, a przy tym są bardziej niezawodne.
- Obsługa dysków SSD.

- Opcjonalna zdalna replikacja: Replikacja danych do innej lokalizacji, która obejmuje mirroring danych.
- Migawki: Łatwo odzyskać pliki po przypadkowym usunięciu lub zmianą z punktu w czasie.
- Kopia dysku wirtualnego (VDC): szybkie i bezproblemowe przenoszenie wirtualnego dysku, tworzenie kopii zapasowych na dysku i odzyskiwanie, replikowanie kopii danych źródłowych.

Zaprojektowano wykorzystanie macierzy dyskowej o parametrach:

1. Zainstalowane dyski SAS:
    a. RAID6 – 12 dysków o prędkości 15k rpm - pojemność około 7,2 TB) – dla potrzeb serwerów produkcyjnych
    b. RAID6 – 15 dysków o prędkości 10k rpm – pojemność około 18 TB – dla potrzeb serwerów produkcyjnych
2. Podwójne kontrolery typu Hot-Swap oferujące w sumie osiem portów FC 16GB
3. Zawartość pamięci cache podtrzymywana za pomocą technologii flash lub bateryjnie przez con najmniej 72h
4. Podwójne zasilacze typu Hot-Swap
5. Możliwość rozbudowy do 180 dysków SAS, NLSAS, SSD

Specyfikacja dla sprzętu:

Macierz dyskowa z kontrolerami FC

Nazwa komponentu	***Wymagane minimalne parametry techniczne***
Obudowa	Do instalacji w standardowej szafie RACK 19”. Wysokość maksymalnie 2U wraz z kompletem szyn do montażu w szafie Rack z możliwością instalacji minimum 24 dysków 2.5” Hot Plug.
Kontrolery	Dwa kontrolery posiadające łącznie minimum osiem portów FC minimum 16 Gb/s wraz z wkładkami SFP do podłączenia serwerów, pracujące w trybie active-active. Wymagane poziomy zabezpieczenia RAID: 0,1,5,6,10. Minimum 4GB na kontroler, pamięć cache zapisu mirrorowana między kontrolerami, z opcją zapisu na dysk lub inną pamięć nieulotną lub podtrzymywana bateryjnie przez min. 72h w razie awarii
Dyski twarde	Zainstalowane dyski :

	12 dysków o pojemności minimum 600GB SAS 15k RPM Hot-Plug 2.5” każdy. 15 dysków o pojemności minimum 1,2TB SAS 10k RPM Hot-Plug 2.5” każdy. Możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych, możliwość obsługi łącznie minimum 180 dysków, wydajnych dysków SAS, SSD, ekonomicznych dysków NearLine SAS, samoszyfrujących dysków SED dostępnych w ofercie producenta macierzy, możliwość mieszania typów dysków w obrębie macierzy oraz półki.
Oprogramowanie	Zarządzające macierzą w tym powiadamianie mailem o awarii, umożliwiające maskowanie i mapowanie dysków. Dostarczyć licencję umożliwiającą: - utworzenie minimum 128 kopii migawkowych per virtual disk i 512 per system. - utworzenie do 512 jednoczesnych wirtualnych kopii dysków. Licencja zaoferowanej macierzy powinna umożliwiać podłączanie minimum 32 hostów bez konieczności zakupu dodatkowych licencji. Zarządzanie macierzą poprzez oprogramowanie zarządzające lub przeglądarkę internetową.
Bezpieczeństwo	Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne. Możliwość przydzielenia większej przestrzeni dyskowej dla serwerów niż fizycznie dostępna (Thin Provisioning) Fizyczne zabezpieczenie dedykowane przez producenta serwera uniemożliwiające wyjęcie dysków twardych umieszczonych na froncie obudowy przez nieuprawnionych użytkowników.
Dokumentacja	Zamawiający wymaga dokumentacji w języku polskim lub angielskim
Certyfikaty	Macierz wyprodukowana zgodnie z normą ISO 9001 oraz 14001 Zgodność z systemami operacyjnymi: Microsoft® Windows®, VMware®, Microsoft Hyper-V®, Citrix® XenServer®, Red Hat® oraz SUSE
Gwarancja	Pięć 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. W przypadku awarii dyski twarde pozostają własnością Zamawiającego. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia.

12.4. Oprogramowanie wirtualizacyjne

Oprogramowanie wirtualizacyjne wykorzystywane będzie na serwerach produkcyjnych w celu wirtualizacji maszyn serwerowych dla nowego środowiska produkcyjnego.

Zaprojektowano platformę, która oferuje usprawnienia w zakresie wirtualizacji, skalowalności oraz wydajności. Platforma ta jest kompleksowym rozwiązaniem dla firm, które chcą wdrożyć wirtualizację serwerów fizycznych, mając jednocześnie pewność utrzymania najwyższej dostępności i ochrony danych. Pakiet ten obejmuje 6 licencji CPU oprogramowania dla 3 serwerów, do 2 procesorów każdy i 1 licencję oprogramowania do zarządzania maszynami wirtualnymi.

Wykonawca musi uwzględnić zwirtualizowanie dotychczasowego środowiska składającego się z dwóch serwerów ficzycznych, na których znajdują się:

- System operacyjny: Windows server 2003 R2; baza danych:Oracle 9 SE; oprogramowanie użytkowe: optimed, optinfzkom, eskulap apteka, KS-pps;
- System operacyjny: Windows server 2008 R2 ; baza danych: firebird; oprogramowanie użytkowe: ERP firmy HEX;

Wirtualizacja ma być podstawą dla tworzonego portalu e-Pacjent, który ma działać w modelu chmury obliczeniowej SaaS.

Do zaprojektowanej licencji należy dokupić 5 letni pakiet serwisowy - Pomoc techniczna dostępna 12 godzin na dobę w godzinach pracy krajowego oddziału od poniedziałku do piątku.

Specyfikacja dla oprogramowania:

Oprogramowanie wirtualizacyjne z przeznaczeniem dla max 3 hostów po max 2 CPU

Nazwa komponentu	***Wymagane minimalne parametry techniczne***
Oprogramowanie do wirtualizacji	Licencje muszą umożliwiać uruchamianie wirtualizacji na serwerach fizycznych o łącznej liczbie 6 procesorów fizycznych oraz jednej konsoli do zarządzania całym środowiskiem. 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 12h na dobę.
Konsolidacja	• 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 bez konieczności nadawania takim osobom bezpośredniego dostępu do głównej konsoli zarządzającej całym środowiskiem. • 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. • 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	• 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 jaki 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	• 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.

12.5. Oprogramowanie operacyjne dla serwerów

Oprogramowanie systemowe wykorzystywane będzie na serwerach produkcyjnych dla nowego środowiska produkcyjnego.
Zaprojektowano: System operacyjny w wersji podstawowej wraz z licencjami dostępowymi lub System operacyjny w wersji podstawowej bez licencji dostępowych o ile producent systemu operacyjnego ich nie wymaga.

Oprogramowanie systemowe wykorzystywane będzie na serwerach produkcyjnych dla nowego środowiska produkcyjnego.
System operacyjny w wersji podstawowej ma umożliwić wdrożenie na macierzy dwóch maszyn wirtualnych na każdą licencję z wykorzystaniem serwerów produkcyjnych. Licencja kupowana jest dla każdej maszyny fizycznej z zainstalowanymi max 2 procesorami fizycznymi.
Wykonawca musi zbudować środowisko w oparciu o system usług katalogowych.

Zaplanowano po dwie licencje na serwery aplikacyjny i bazodanowy oraz jedną licencję na serwer backupu.

Nazwa	*Ilość*
System operacyjny w wersji podstawowej	5
Licencje dostępowe	170

Specyfikacja istotnych warunków zamówienia dla oprogramowania:

Licencja na oprogramowanie serwerowe

Nazwa komponentu	***Wymagane minimalne parametry techniczne***
Wykonawca dostarczy 5 licencji na serwerowy system operacyjny wraz z licencjami umożliwiającymi korzystanie z funkcji systemu przez 170 urządzeń komputerowych.	
Liczba rdzeni procesorów i ilość pamięci nie mogą mieć wpływu na liczbę oferowanych licencji. Licencja ma uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym lub dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.	
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: – 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	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	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: – Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, – Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, – Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. – Zdalna dystrybucja oprogramowania na stacje robocze. – Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej – Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: Dystrybucję certyfikatów poprzez http

	Konsolidację CA dla wielu lasów domeny, Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen. Szyfrowanie plików i folderów. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). – Posiada możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów. – Serwis udostępniania stron WWW. – Wsparcie dla protokołu IP w wersji 6 (IPv6), – Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, – Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie 1000 aktywnych środowisk wirtualnych systemów operacyjnych. 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) 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.
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.

28	System musi posiadać wspeierać usługikatalogowe o następujących cechach: – muszą zapewniać zarządzanie posiadanymi przez zamawiającego usługami sieciowymi na platformach NetWare i Open Enterprise Server – zgodne ze standardem LDAPv3 określonym w stosownych dokumentach RFC. Zgodność ta musi być potwierdzona certyfikatem niezależnej organizacji testującej (np. certyfikaty LDAP Certified i LDAP Certified v.2 organizacji The Open Group/The Open Brand) – muszą mieć możliwość uruchamiania instancji nie tylko na oferowanym systemie operacyjnym serwera ale także na innych platformach systemowych tj. Microsoft Windows, Linux, Solaris, AIX i HP-UX. – muszą być wyposażone w oprogramowanie umożliwiające dwukierunkową synchronizację danych (np. kont użytkowników, haseł itd.) z innymi usługami katalogowymi tj. Microsoft Active Directory, Novell NDS – muszą być zarządzane w stopniu zaawansowanym (tj. umożliwiać: zakładanie, usuwanie, modyfikowanie kont użytkowników, ich uprawnień, haseł) z poziomu przeglądarki internetowej – muszą być zintegrowane z systemem plików serwera w celu zarządzania uprawnieniami do danych dla użytkowników zdefiniowanych w usłudze katalogowej. Dla przechowywanych danych system operacyjny musi posiadać system plików o następujących cechach: – musi umożliwiać użytkownikowi (bez udziału administratora systemu) odzyskanie skasowanych danych – musi umożliwiać bezpieczne skasowanie danych poprzez fizyczne zamazanie rekordów na nośniku, uniemożliwiające odtworzenie tych danych za pomocą oprogramowania do odzyskiwania danych (wymagania bezpieczeństwa przechowywanych danych) – musi obsługiwać kompresję i szyfrowanie przechowywanych danych – musi obsługiwać zarządzanie uprawnieniami do plików i katalogów dla użytkowników zdefiniowanych w usłudze katalogowej.

12.6. Biblioteka taśmowa z jednym napędem LTO-6

Regularne tworzenie kopii zapasowych według ustalonych wytycznych jest bardzo ważnym elementem pełnej strategii umożliwiającej odtworzenie danych w przypadku awarii. Biblioteka taśmowa ułatwia zautomatyzowanie procesu tworzenia kopii zapasowych. Zaprojektowana biblioteka to urządzenie o wielkości 2U. Obsługuje maksymalnie 2 napędy LTO i 24 gniazda na taśmy.

Taśmy mogą być importowane lub eksportowane pojedynczo przez szczelinę lub w zestawach po 12 sztuk, umieszczonych w jednym lub dwóch magazynkach. Do określania położenia nośników taśmowych w bibliotece wykorzystywana jest technologia skanowania kodów kreskowych.

Wbudowany, przyjazny w obsłudze interfejs LCD ułatwia operatorowi monitorowanie, konfigurowanie i serwisowanie biblioteki oraz sterowanie jej pracą. Gdy operator jest poza biurem, może zdalnie zarządzać wszystkimi funkcjami biblioteki taśmowej: przeprowadzania diagnostyki, sprawdzania informacji o stanie, monitorowania wykonywanych operacji, śledzenia dzienników oraz aktualizacji oprogramowania wewnętrznego.

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

Specyfikacja dla sprzętu:

Nazwa komponentu	*Wymagane minimalne parametry techniczne*
Obudowa	Do zamontowania w szafie rack, maksymalnie 4U, wbudowany czytnik kodów kreskowych.
Napęd	1x LTO6
Interfejs	1 x SAS 6Gb/s
Liczba slotów	24 w tym minimum jeden slot we/wy, jeżeli licencjonowana jest liczba slotów - wymagane aktywowanie wszystkich slotów W komplecie 15 sztuk taśm LTO6 oraz 10 sztuk taśm WORM i 1 szt. taśma czyszcząca oraz etykiety dla min. 60 taśm.
Dodatkowe	– Interfejs do zarządzania poprzez przeglądarkę WWW oraz możliwość zarządzania bezpośrednio z użyciem wbudowanych klawiszy i wyświetlacza LCD – Wyjmowalne magazynki kieszeni na taśmy w celu łatwego zarządzania większą ilością taśm – Wsparcie dla nośników LTO WORM (Write Once, Read Many), umożliwiających spełnienie norm prawnych dotyczących odpowiednio długiego przechowywania nienaruszonych danych (archiwizacja) – Obsługa SNMP oraz IP6 Wsparcie dla technologii szyfrowania backupowanych danych
Gwarancja	Pięć lat gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 8x5 w dni robocze poprzez ogólnopolską linię telefoniczną producenta. – W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych). – Firma serwisująca musi posiadać ISO 9001:2000 na

	świadczenie usług serwisowych oraz posiadać autoryzacje producenta serwera.

12.7. Oprogramowanie do backupu

Planowany pakiet oprogramowania do backupu jest przeznaczony dla małych firm ze środowiskami obejmującymi 2, 4 lub 6 gniazd procesorów. Zapewnia wszystkie elementy funkcji ochrony danych klasy korporacyjnej:

- Szybkie odzyskiwanie - umożliwia szybkie odzyskanie dowolnych danych — całej maszyny wirtualnej, wybranego pliku lub elementu aplikacji
- Unikanie utraty danych - ciągła ochrona danych i usprawnione funkcje odzyskiwania awaryjnego
    - 2-in-1: backup and replication
- Pewność ochrony – Zaimplementowane funkcje dają gwarancję, że w razie potrzeby będzie można pomyślnie przywrócić pliki, aplikacje i serwery wirtualne.
- Pełny wgląd - Dzięki wykorzystaniu funkcji i możliwości planowanego rozwiązania umożliwia ono aktywne monitorowanie i ostrzeganie przed problemami, zanim wpłyną one na działalność operacyjną.
    - Całodobowe monitorowanie i ostrzeganie w czasie rzeczywistym
    - W pełni konfigurowalne raporty

Dla potrzeb backupu dobrano oprogramowanie do wykonywania kopii zapasowych maszyn wirtualnych w środowisku planowanego wirtualizatora (bez backupu serwerów fizycznych)

Specyfikacja dla oprogramowania:

Nazwa komponentu	*Wymagane minimalne parametry techniczne*
Licencje muszą umożliwiać backup maszyn wirtualnych na serwerach fizycznych o łącznej liczbie 6 procesorów fizycznych. Licencja przeznaczona dla wykorzystywanego przez Wykonawcę środowiska wirtualizacji. Wszystkie licencje powinny być dostarczone wraz z 3-letnim wsparciem, świadczonym przez producenta oprogramowania, które powinno umożliwiać zgłaszanie problemów 5 dni w tygodniu przez 8h na dobę.	
• Oprogramowanie powinno współpracować z instrastrukturą 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 Manger oraz z hostami niezarządzanymi • Oprogramowanie powinno zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V	
• 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 wirtualych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)

- Oprogramowanie powinno wykorzystywać VMware vStorage API for Data Protection i używać mechanizmów Change Block Tracking
- 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 kopiowania
- Oprogramowanie powinno mieć możliwość replikacji wirtualnych maszyn pomiędzy lokalizacjiami

Funkcjonalność ta powinna być zapewniona dla vSphere i Hyper-V

- 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 vSphere
- 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 srodowiska 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 umozliwić odtworzenie plików na maszyne 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
  - **BSD**
    - UFS, UFS2
  - **Solaris**
    - ZFS
  - **Mac**
    - HFS, HFS+
  - **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 umożliwość weryfikację odtwarzalności dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzgędniać możliwość uruchomienia dowonego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie.
- Oprogramowanie powinno mieć podobne mechanizmy dla replik w środowisku vSphere.

12.8. Szafa serwerowa z wyposażeniem

W pomieszczeniu Podstawowej Serwerowni zostanie zainstalowana jedna szafa serwerowa o wysokości 42U i wymiarach 800x1000.
W szafie tej zostanie zainstalowane wyposażenie części produkcyjnej: serwery aplikacyjny i bazodanowy, macierz, przełączniki LAN, zasilacz awaryjny UPS.
W drugiej szafie rack w pomieszczeniu drugiej Serwerowni zamontowane zostaną pozostałe urządzenia: serwer kopii zapasowej, biblioteka taśmowa, przełączniki dostępowe LAN itp..

Szafa zostanie dostarczona z następującym wyposażeniem (lub równoważne) – 2 komplety:

- Szafa serwerowa z możliwością rozkręcenia (nie dopuszcza się szaf spawanych) o wymiarach:
  - szerokość: 800 mm, głębokość: 1000 mm, wysokość: 42U)
- Rodzaj drzwi i osłon bocznych:
  - drzwi przednie drzwi blaszane z perforacją typu A
  - drzwi tylne drzwi blaszane z perforacją typu A
  - lewy bok osłona blaszana pełna
  - prawy bok osłona blaszana pełna
- Rodzaj dachu i podstawy
  - dach z otworami pod zaślepki
- podstawa cokół o wysokości 100 mm wraz z zespołem ramy wsporczej do cokołu 800x1000
- dwie pary belek nośnych 19" oraz jedna para belek nośnych środkowych
- listwa zasilająca 9 gniazdowa
- panel wentylacyjny dachowy czterowentylatorowy

Specyfikacja dla szafy:

Nazwa komponentu	***Wymagane minimalne parametry techniczne***
Obudowa RACK	Szafa przeznaczona do zastosowania wewnątrz pomieszczeń o wymiarach: szerokość: 800 mm, głębokość: 1000 mm, wysokość: 42U Szafa z możliwością rozkręcenia, rozłożenia i ponownego złożenia Rodzaj drzwi i osłon bocznych: drzwi przednie - drzwi blaszane z perforacją typu A drzwi tylne - drzwi blaszane z perforacją typu A lewy bok - osłona blaszana pełna

	prawy bok - osłona blaszana pełna Rodzaj dachu i podstawy dach z otworami pod zaślepki podstawa cokół o wysokości 100 mm Cokół z wysuwaną ramą wsporczą Trzy pary belek nośnych 19" Kolor szafy RAL 9005 (czarny)
Wyposażenie dodatkowe	Półka stała o głębokości min. 620 mm mocowana na 4 belkach nośnych, RAL 9005 - czarna Listwa zasilająca 1 x 16A, (montaż 19") - 9 gniazd z bolcem Panel wentylacyjny dachowy czterowentylatorowy z termostatem, RAL 9005

12.9. Przełącznik KVM+KMM

Przełącznik KVM to moduł sterujący, który zapewnia bezpieczny dostęp bezpośrednio do 8 komputerów z jednej konsoli (tj. klawiatury, monitora i myszy). Moduł ten, zajmujący wysokość 1U w stelażu, ma wysuwaną konstrukcję i obejmuje zintegrowany monitor LCD, klawiaturę i touchpad. Ekran LCD i klawiatura/touchpad wysuwają się niezależnie względem siebie.
Zaprojektowany przełącznik zapewnia łączność opartą na protokole IP, dzięki czemu operatorzy lokalny i zdalny mogą monitorować komputery w ramach danej instalacji i uzyskiwać do nich dostęp. Ponieważ KVM działa na bazie protokołu komunikacyjnego TCP/IP, można do niego uzyskać dostęp z dowolnego komputera w sieci LAN, WAN lub Internet-u.

Kompaktowe i gęsto upakowane złącza RJ-45 i obsługa przewodów Cat 5e/6 zapewniają wygodne i uporządkowane okablowanie stanowiska. Przewody-adaptery KVM zapewniają łączność z komputerami oraz umożliwiają tworzenie dowolnych kombinacji komputerów PC, Mac i Sun w ramach jednej instalacji.

Wraz z przełącznikami (jeden zamontowany w szafie serwerowej w podstawowej serwerowni, drugi zamontowany w szafie serwerowej w drugiej serwerowni) należy dostarczyć odpowiednią ilość kabli przyłączeniowych do nowoprojektowanych serwerów oraz do istniejących.

Przykładowa dla KVM + KMM:

Nazwa komponentu	*Wymagane minimalne parametry techniczne*
Obudowa	Max. 1U do montażu w szafie rack

Złącza	Porty konsoli: – Klawiatura: USB – Mysz: USB – Grafika: HDB-15 Porty KVM: 8 x RJ-45 Zasilanie: gniazdo AC Uaktualnianie oprogramowania: RJ-11 Mysz zewnętrzna: USB LAN: RJ-45
Matryca	Min. LCD 17”, 1280 x 1024
Funkcjonalność	– Kontrolowanie do 8 komputerów za pomocą jednej konsoli – Osobna magistrala do zdalnego dostępu na zasadzie KVM over IP – Adaptery KVM zapewniające automatyczną konwersję i współpracujące z różnymi kombinacjami interfejsów (PS/2, USB, Sun, szeregowe) i różnymi typami komputerów – Obsługa zewnętrznej myszy USB – Możliwość wysuwania się monitora LCD niezależnie od klawiatury/touchpada – Możliwość uchylania monitora do min. 120 stopni w celu dobrania najlepszego kąta patrzenia – możliwość zablokowania szuflady konsoli na czas nieużywania jej
Zarządzanie	– Obsługa min. 32 użytkowników zdalnych zalogowanych jednocześnie – Możliwość zakończenia dowolnie działającej sesji
Zabezpieczenia	– Obsługa zdalnego uwierzytelniania: RADIUS, LDAP, LDAPS oraz MS Active Directory – 128-bitowe szyfrowanie SSL zabezpieczające hasło podczas logowania – Obsługa filtra IP/MAC zapewniającego zaawansowaną ochronę – Możliwość konfigurowania uprawnień użytkowników i grup do uzyskiwania dostępu do serwerów
Wyposażenie	– 1 x przewód zasilający – 1 x zestaw do montażu w szafir rack – 4 x Przewód-adapter KVM USB
Gwarancja	24 miesiące z czasem reakcji w następnym dniu roboczym

12.10. Zasilanie awaryjne UPS do serwerów

W celu zabezpieczenia serwerów i macierzy przed krótkotrwałymi zanikami napięcia zaprojektowano zastosowanie zasilaczy awaryjnych UPS – po jednej sztuce dla każdej szafy serwerowej.

Zasilacze te posiadają konstrukcję line-interactive, z technologią automatycznej regulacji obniżania/podnoszenia napięcia. Technologia ta chroni przed wahaniami napięcia sieciowego poprzez jego podwyższanie lub obniżanie do poziomu wymaganego przez podłączone urządzenie. Umożliwia też wydłużenie czasu pracy akumulatora przez optymalizację czasu pracy na zasilaniu sieciowym przed przełączeniem na zasilanie akumulatorowe.

UPS-y te posiadają się między innymi poniższe cechy:

- Zabezpieczenie przeciwprzepięciowe linii danych
- Wczesne ostrzeganie o stanie zasilacza UPS
- Pełne sekwencyjne testowanie akumulatorów
- Zabezpieczenie przeciwprzepięciowe
- Zdalne awaryjne wyłączanie zasilania
- Możliwość wymiany akumulatorów przez użytkownika podczas pracy urządzenia
- Długi czas akumulatorowego zasilania awaryjnego przy pełnym obciążeniu w razie awarii zasilania sieciowego, umożliwiający kontrolowane wyłączenie podłączonych urządzeń
- Gniazda wyjściowe:
  - (6) IEC-320-C13
  - (1) IEC-320-C19
- Kształt napięcia przy pracy akumulatorowej: sinusoida

Zasilanie elementów serwerowych kluczowych i pozostałe urządzenia serwerowe proponujemy podłączyć w następujący sposób (dwa tory zasilania):

- jeden z zasilaczy pozostałych urządzeń podłączymy do PDU/listwy zasilającej, zaś PDU/listwę zasilającą podłączamy do UPS-a zasilacza awaryjnego UPS – dedykowany obwód z rozdzielni komputerowej.
- drugi zasilacz pozostałych urządzeń podłączamy do listwy PDU/listwy zasilającej, zaś listwę PDU/zasilajacą podłączamy do dedykowanego obwodu z rozdzielni komputerowej - bez podtrzymywania awaryjnego.

Układ taki uchroni nas przed awarią zasilania pozostałych urządzeń (od strony zaniku napięcia), a także w momencie uszkodzenia UPS-a będziemy nadal mieć zasilanie bezpośrednio z rozdzielni komputerowej.

Specyfikacja dla sprzętu:

Nazwa komponentu	*Wymagane minimalne parametry techniczne*
Moc pozorna	Min. 3000VA
Moc rzeczywista	Min. 2700W
Architektura	line-interactive
Obudowa	Max. 2U do montażu w szafie rack
Gniazda wejściowe	Min. 1 x IEC-320-C20
Gniazda wyjściowe	Min. 6 x IEC-320-C13 i 1 x IEC-320-C19
Czas podtrzymania przy obciążeniu 50%	Min. 13 min.
Czas podtrzymania dla	Min. 5 min.

obciążenia 100%	
Czas przełączania	Max. 6ms
Gniazda komunikacyjne	RS232, USB, slot na kartę rozszerzeń wyposażony w kartę SNMP
Dodatkowe funkcjonalności	Zabezpieczenie przeciwprzepięciowe linii danych Wczesne ostrzeganie o stanie zasilacza UPS Pełne sekwencyjne testowanie akumulatorów Zdalne awaryjne wyłączanie zasilania
Sygnalizacja	Diodowy system sygnalizacji informujący min. o: Praca z sieci zasilającej Konieczna wymiana baterii Praca z baterii Przeciążenie UPS-a Dźwiękowy system sygnalizacji.
Oprogramowanie do zarządzania	Dedykowane przez producenta oprogramowanie do zarządzania umożliwiające wyłączenie serwera w przypadku dużego rozładowania akumulatorów.
Wyposażenie	Podręcznik użytkownika na płycie CD z oprogramowaniem, kabel szeregowy DB9, kabel USB, podstawa do montażu wolnostojącego, uchwyty do montażu w szafie wraz z elementami montażowymi
Rozszerzenie czasu podtrzymania	Możliwość podłączenia dodatkowych modułów bateryjnych
Gwarancja	3 lata na urządzenie i baterię w miejscu instalacji z czasem reakcji w następnym dniu roboczym

12.11. Zasilanie awaryjne UPS do Punktów Dystrybucyjnych

W celu zabezpieczenia przełączników sieciowych przed krótkotrwałymi zanikami napięcia zaprojektowano zastosowanie zasilaczy awaryjnych UPS – po jednej sztuce dla każdej szafy dystrybucyjnej.

Zasilacze te posiadają konstrukcję line-interactive, z technologią automatycznej regulacji obniżania/podnoszenia napięcia. Technologia ta chroni przed wahaniami napięcia sieciowego poprzez jego podwyższanie lub obniżanie do poziomu wymaganego przez podłączone urządzenie. Umożliwia też wydłużenie czasu pracy akumulatora przez optymalizację czasu pracy na zasilaniu sieciowym przed przełączeniem na zasilanie akumulatorowe.

UPS-y te posiadają się między innymi poniższe cechy:

- Zabezpieczenie przeciwprzepięciowe linii danych
- Wczesne ostrzeganie o stanie zasilacza UPS
- Pełne sekwencyjne testowanie akumulatorów

- Zabezpieczenie przeciwprzepięciowe
- Zdalne awaryjne wyłączanie zasilania
- Możliwość wymiany akumulatorów przez użytkownika podczas pracy urządzenia
- Gniazda wyjściowe:
    - (8) IEC-320-C13
- Kształt napięcia przy pracy akumulatorowej: sinusoida

Specyfikacja dla sprzętu:

Nazwa komponentu	*Wymagane minimalne parametry techniczne*
Moc pozorna	Min. 1500VA
Moc rzeczywista	Min. 1350W
Architektura	line-interactive
Obudowa	Max. 2U do montażu w szafie rack
Gniazda wejściowe	Min. 1 x IEC-320
Gniazda wyjściowe	Min. 8 x IEC-320-C13
Czas podtrzymania przy obciążeniu 50%	Min. 8,5 min.
Czas podtrzymania dla obciążenia 100%	Min. 2,9 min.
Czas przełączania	Max. 6ms
Gniazda komunikacyjne	RS232, USB, slot na kartę rozszerzeń wyposażony w kartę SNMP
Dodatkowe funkcjonalności	Zabezpieczenie przeciwprzepięciowe linii danych Wczesne ostrzeganie o stanie zasilacza UPS Pełne sekwencyjne testowanie akumulatorów Zdalne awaryjne wyłączanie zasilania
Sygnalizacja	Diodowy system sygnalizacji informujący min. o: Praca z sieci zasilającej Konieczna wymiana baterii Praca z baterii Przeciążenie UPS-a Dźwiękowy system sygnalizacji.
Oprogramowanie do zarządzania	Dedykowane przez producenta oprogramowanie do zarządzania umożliwiające wyłączenie serwera w przypadku dużego rozładowania akumulatorów.
Wyposażenie	Podręcznik użytkownika na płycie CD z oprogramowaniem, kabel USB, uchwyty do montażu w szafie wraz z elementami montażowymi
Gwarancja	3 lata na urządzenie i baterię w miejscu instalacji z czasem reakcji w następnym dniu roboczym

12.12. System Monitorowania Infrastruktury

System Monitorowania Infrastruktury musi być wdrożony na serwerze Zamawiającego. Obejmować musi monitorowanie wszystkich urządzeń: serwerów, macierzy, biblioteki,

przełączników sieciowych, kontrolera WiFi oraz punktów dostępowych, wskazanych stacji roboczych.
Dodatkowo musi monitorować usługi sieciowe, takie jak:

- SMTP, POP3, http, NNTP, ping
- Serwerów pocztowych
- Monitorowania serwerów WWW i adresów URL
- Monitor usług działających w ramach systemu Windows
- Monitorowanie zasobów hosta (obciążenie CPU, użycie dysku, itp)
- Monitorowanie wydajności systemów Windows (obciążenie CPU, pamięci, zajętości dysków)

Wdrożenie musi także obejmować moduł inwentaryzacji sprzętu, który musi umożliwiać prowadzenie bazy ewidencji majątku IT.

Specyfikacja dla oprogramowania:

Oprogramowanie musi posiadać budowę modułową, składać się z serwera zarządzającego oraz modułów zdalnych.
Moduły muszą umożliwiać kompleksowy monitoring sieci oraz monitoring sprzętu komputerowego.
Konsola dostępna poprzez dowolna przeglądarkę www.
W zakresie obsługi sieci program musi pozwalać na wyświetlenie konfiguracji oraz jej prezentację.
Program musi umożliwiać monitorowanie nielimitowanej liczby urządzeń sieciowych.
Monitorowanie infrastruktury musi obejmować między innymi serwery Windows, Linux, Unix oraz routery, przełączniki, VOIP i firewall w zakresie:

- Monitorowanie usług sieciowych (SMTP, POP3, http, NNTP, ping). Musi umożliwiać monitorowanie czasu ich odpowiedzi i procent utraconych pakietów.
- Monitorowanie komponentów serwerowych (przełączniki, routery, czujniki temperatury i wilgotności, etc.)
- Serwerów pocztowych: program monitoruje zarówno serwis odbierający, jak i wysyłający pocztę.
- Monitorowania serwerów WWW i adresów URL
- Monitor usług działających w ramach systemu Windows
- Monitorowanie zasobów hosta (obciążenie CPU, użycie dysku, itp)
- Monitorowanie wydajności systemów Windows (obciążenie CPU, pamięci, zajętości dysków)

Program musi posiadać możliwość monitorowania stanu systemów i wysyłania powiadomienia (do wskazanych osób kontaktowych) w razie gdy przestały one odpowiadać lub gdy monitorowane ważne parametry znajdują się poza określonym zakresem zdefiniowanym przez administratora.
Program musi posiadać możliwość wysyłania powiadomień, nawet jeśli serwer pocztowy nie działa.

Program musi umożliwiać rysowanie dynamicznych Map sieci, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie.
Obsługa szyfrowania SSL w powiadomieniach e-mail.
Obsługa urządzeń SNMP (przełączniki, routery, drukarki sieciowe, urządzenia VoIP).
Powiadomienia mailowe w razie problemów z urządzeniami sieciowymi.
Usługa wdrożeniowa systemu monitorowania musi obejmować instalację i konfigurację co wszystkich hostów w sieci i z nimi związanych monitorowanych usług.

Moduł inwentaryzacji sprzętu musi umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu.
Dostępny agent na system Android oraz systemy Windows.
Inwentaryzacja oprogramowania musi zapewniać funkcjonalność w zakresie pozyskiwania informacji o posiadanym oprogramowaniu oraz posiadanych licencjach.
Moduł inwentaryzacji musi tworzyć zbiór podłączonych urządzeń do komputerów oraz mieć możliwość generowania raportów do pliku xml.
Usługa wdrożeniowa modułu inwentaryzacji musi obejmować instalację i konfigurację co najmniej 150 agentów.

5. Sprzęt komputerowy i peryferia

5.1. Komputer stacjonarny. Typu All in One, komputer wbudowany w monitor oraz oprogramowaniem systemowym i oprogramowaniem antywirusowym – 110 szt.

Komputer stacjonarny – procesor dwurdzeniowy czterowątkowy, 8GB DDR3, 500GB (lub 120GB SSD) HDD, Grafika zintegrowana, system operacyjny w wersji PRO, 3 lat gwarancji

Specyfikacja dla sprzętu:

Nazwa komponentu	*Wymagane minimalne parametry techniczne*
Typ	Komputer stacjonarny. Typu All in One, komputer wbudowany w monitor. W ofercie wymagane jest podanie modelu producenta komputera.
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna
Wydajność obliczeniowa	**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 1480 punktów, Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rodzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów Oferent musi dostarczyć Zamawiającemu oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego
Procesor	Procesor wielordzeniowy ze zintegrowaną grafiką, osiągający w teście PassMark CPU Mark wynik min. 5350 punktów , załączyć do oferty wyniki przeprowadzonego testu
Pamięć operacyjna RAM	8GB DDR3 1600MHz non-ECC możliwość rozbudowy do min 16GB
Parametry pamieci masowej	Min. 128 GB SATA wykonany w technologi Solid-state drive
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 980 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/m² / min. 600:1
	Głębia koloru	16.7mln
	Response time	max. 25 msec
	Odświeżanie	min. 60 Hz
	Kąty Horizontal/Vertical	min. 89 / 89
	Rodzaj matrycy	typu Non-touch (Anti-Glare)
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, 24-bitowa konwersja sygnału cyfrowego na analogowy i analogowego na cyfrowy np. Realtek ALC3661 lub równoważna; wbudowane dwa głośniki min. 2,W na kanał (moment szczytowy 3W)	
Obudowa	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), Demontaż standu musi odbywać się bez użycia narzędzi, mocowanie standu opatrzone w przycisk zwalniający. 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, Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS. Zasilacz wewnętrzny o mocy max. 155W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100% Zasilacz w oferowanym komputerze musi się znajdować na stronie http://www.plugloadsolutions.com/80pluspowersupplies.aspx, do oferty należy dołączyć wydruk potwierdzający spełnienie wymogu 80plus, w przypadku kiedy u producenta występuje kilka zasilaczy które są montowane na etapie produkcji w fabryce załączyć wydruki dla wszystkich zasilaczy. Wydruki 80plus musza być potwierdzone przez producenta lub dołączone oświadczenie producenta komputera iż wskazane zasilacze przez wykonawcę spełniają 80plus. 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). Obudowa musi posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym. Wbudowany wizualny system diagnostyczny włączniku 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: - uszkodzenie lub brak pamięci RAM - uszkodzenie płyty głównej [w tym również portów I/O, chipset] - uszkodzenie kontrolera Video - awarię BIOS'u - awarię procesora Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk 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. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS.
Zgodność z systemami operacyjnymi i standardami	Potwierdzenie kompatybilności komputera na daną platformę systemową (wydruk ze strony)
Bezpieczeństwo	Wbudowany, czyli wlutowany (nie dopuszcza się zintegrowanych z płytą główną tzn. układ wykorzystujący jakiekolwiek 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. Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot'owania, umożliwiający jednoczesne przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. System opatrzony min. o funkcjonalność : - 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 Zasilacz wyposażony swój własny system diagnostyczny niezależny od pozostałych komponentów oferowanego komputera umożliwiający sprawdzenie poprawnego funkcjonowania zasilacza bez narażania pozostałych składowych na ewentualne uszkodzenia (przepięcia itp.) Czujnik otwarcia obudowy musi zbierać logi i zapisywać je w BIOS
Wirtualizacja	Sprzętowe wsparcie technologi wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu).
BIOS	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. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: ▪ 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 osiąganej prędkości zainstalowanego procesora, ▪ maksymalnej osiąganej 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 technologi 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, ▪ 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 haśle administratora i/lub zdefiniowanym haśle dla dysku Twardego. Użytkownik po wpisaniu swojego hasła jest wstanie 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 błędu 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 napięcia [funkcja związana z architekturą procesora, nie dopuszcza się overclokingu, 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 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 : - 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 :

	- minimalnej – następuje skrócony czas rozruchu komputera z pominięciem pełnej weryfikacji inicjalizacji konfiguracji sprzętowej - gruntownej - podczas rozruchu komputera następuje pełna weryfikacja i inicjalizacja konfiguracji sprzętowej, • 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. : - 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

	- 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: - 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	• Certyfikat ISO9001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu) • Deklaracja zgodności CE (załączyć do oferty) • Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych", pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram • Komputer musi spełniać wymogi normy Energy Star 6.0 lub dołączony do oferty certyfikat potwierdzony przez producenta Wymagany wpis dotyczący oferowanego komputera w internetowym katalogu http://www.eu-energystar.org lub http://www.energystar.gov – dopuszcza się wydruk ze strony internetowej
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 (załączyć oświadczenie producenta wraz z raportem badawczym wystawionym przez niezależną akredytowaną jednostkę)
Warunki gwarancji	3-letnia gwarancja producenta świadczona na miejscu u klienta, W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego – wymagane jest dołączenie do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu o spełnieniu tego warunku. Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta – wymagane dołączenie do oferty oświadczenia Producenta potwierdzonego, że serwis

	będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta
Wsparcie techniczne producenta	Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera – do oferty należy dołączyć link strony.
System Operacyjny	Zainstalowany system operacyjny Windows 10 Professional, 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),
Złącza i porty	Wbudowane porty: • 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 : 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	Dołączone do oferowanego komputera oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające : - 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 : a. o poprawkach i usprawnieniach dotyczących aktualizacji b. dacie wydania ostatniej aktualizacji c. priorytecie aktualizacji d. zgodność z systemami operacyjnymi e. jakiego komponentu sprzętu dotyczy aktualizacja f. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e. - 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 rozbiciem 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.

W celu zabezpieczenia sieci firmowej przed złośliwymi wirusami, proponujemy użycie pakietu ochrony na 3 lata zawierającego:

- Ochronę komputerów
  - 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
  - Zoptymalizowany dla środowiska wirtualnego
  - Pełne wsparcie dla środowisk klastrowych
  - Skanowanie przechowywanych plików
  - Wyspecjalizowane narzędzie czyszczące
- Centralne zarządzanie
  - Wsparcie dla wielu platform - Działa na systemach Windows i Linux. Umożliwia instalację wszystkich komponentów podczas instalacji domyślnej lub wybór najpotrzebniejszych elementów. Umożliwia instalację jako urządzenie wirtualne.
  - Niezależne agenty - Niezależny agent uruchamia wszystkie zadania, polityki i wydarzenia bezpośrednio na stacji roboczej, nawet bez połączenia z konsolą zdalnego zarządzania.
  - 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.

Specyfikacja dla sprzętu:

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. 4. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim. 5. Skuteczność programu potwierdzona nagrodami VB100 i AV-comparatives.
Ochrona antywirusowa i antyspyware	1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 3. Wbudowana technologia do ochrony przed rootkitami. 4. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 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. 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. 8. 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). 9. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 10. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. 11. Możliwość skanowania dysków sieciowych i dysków przenośnych. 12. Skanowanie plików spakowanych i skompresowanych. 13. Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (w tym z uwzględnieniem plików bez rozszerzeń). 14. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.

15. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
16. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
17. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.
18. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
19. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
20. 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.
21. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego).
22. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
23. 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).
24. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
25. Możliwość definiowania różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie.
26. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
27. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
28. 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. 29. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora. 30. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 31. Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie. 32. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 33. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. 34. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta. 35. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego. 36. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 37. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym. 38. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego. 39. 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. 40. 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. 41. 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.

42. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.
43. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
44. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
45. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
46. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.
47. 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.
48. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
49. 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.
50. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
51. 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.
52. System antywirusowy uruchomiony z płyty

	bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku. 53. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym. 54. 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. 55. 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. 56. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia, dana funkcjonalność musi pozwalać na automatyczne wypełnienie właściwości urządzenia dla tworzonej reguły. 57. 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. 58. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 59. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. 60. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika 61. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). 62. 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.

63. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
64. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
65. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
66. Program musi być wyposażona w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp.
67. 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.
68. 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.
69. 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.
70. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
71. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu

	komputera). Każde zadanie może być uruchomione z własnymi ustawieniami. 72. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur. 73. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji. 74. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http 75. Program musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback). 76. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa). 77. Program ma być w pełni zgodny z technologią CISCO Network Access Control. 78. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym. 79. 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. 80. Użytkownik ma mieć możliwość skonfigurowania programu tak aby automatycznie program włączał powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym po określonym przez użytkownika czasie. 81. 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. 82. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. 83. Program musi posiadać możliwość utworzenia z poziomu interfejsu aplikacji dziennika diagnostycznego na potrzeby pomocy technicznej.

	84. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline. 85. Możliwość podejrzenia licencji za pomocą, której program został aktywowany.
Ochrona serwera plików Windows	1. Wsparcie dla systemów: Microsoft Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2, 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 definiowania listy rozszerzeń plików, które mają być skanowane (z uwzględnieniem plików bez rozszerzeń). 15. Możliwość umieszczenia na liście wyłączeń ze

	skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 16. Program musi posiadać funkcjonalność pozwalającą na ograniczenie wielokrotnego skanowania plików w środowisku wirtualnym za pomocą mechanizmu przechowującego informacje o przeskanowanym już obiekcie i współdzieleniu tych informacji z innymi maszynami wirtualnymi. 17. Aplikacja powinna wspierać mechanizm klastrowania. 18. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). 19. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS. 20. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 21. Program ma umożliwiać użytkownikowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, płyt CD/DVD i pamięci masowych FireWire. 22. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model i wersję modelu urządzenia. 23. Aplikacja musi posiadać funkcjonalność, która automatycznie uzupełni elementy wymagane dla tworzenia reguł w oparciu o informacje dostępne z aktualnie podłączonego nośnika. 24. 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. 25. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 26. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. 27. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 28. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym

	dodaniem kolejnych wyłączeń w systemie ochrony. 29. Dodanie automatycznych wyłączeń nie wymaga restartu serwera. 30. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych. 31. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji. 32. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione. 33. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego. 34. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line). 35. 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. 36. 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. 37. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów. 38. Aktualizacje modułów analizy heurystycznej. 39. 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. 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. Wysyłanie zagrożeń do laboratorium ma być możliwe z serwera zdalnego zarządzania i lokalnie z każdej stacji roboczej w przypadku komputerów mobilnych. 42. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają

	być w pełni anonimowe. 43. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. 44. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail. 45. Interfejs programu ma oferować funkcję pracy w trybie bez grafiki gdzie cały interfejs wyświetlany jest w formie formatek i tekstu. 46. Interfejs programu ma mieć możliwość automatycznego aktywowania trybu bez grafiki w momencie, gdy użytkownik przełączy system Windows w tryb wysokiego kontrastu. 47. 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. 48. 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. 49. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo. 50. System antywirusowy ma być w pełni zgodny z technologią CISCO NAC. 51. 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. 52. System antywirusowy ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Program ma także posiadać opcję dezaktywacji tego mechanizmu. 53. 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. 54. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną

	aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku. 55. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym. 56. Program powinien umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: stacji dyskietek, napędów CD/DVD oraz portów USB. 57. 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. 58. 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. 59. 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. 60. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń. 61. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP). 62. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. 63. 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). 64. 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. 65. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają

	wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 66. Praca programu musi być niezauważalna dla użytkownika. 67. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania. 68. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
Administracja zdalna	1. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2003, 2008, 2012 oraz systemach Linux. 2. Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL. 3. Serwer administracyjny musi oferować możliwość wykorzystania już istniejącej bazy danych MS SQL lub MySQL użytkownika. 4. 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. 5. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej. 6. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy występujące w sieci. 7. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6. 8. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający. 9. Zmiana języka panelu administracyjnego nie może wymagać zatrzymania lub reinstalacji oprogramowania zarządzającego. 10. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL. 11. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci. 12. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych. 13. Jeden centralny serwer centralnego zarządzania bez względu na wielkość sieci. 14. Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w

przypadku rozproszonych sieci –serwer pośredniczący (proxy) lub serwer centralny.
15. Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym.
16. Serwer proxy musi być wyposażony we własną bazę danych, w której będą przechowywane dane z agentów na wypadek braku połączenia z serwerem centralnym.
17. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.
18. 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.
19. Serwer http proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) najczęściej pobieranych elementów.
20. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
21. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.
22. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na stacjach roboczych z systemami Windows, Mac OS X oraz Linux.
23. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na urządzeniach mobilnych z systemem Android.
24. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.
25. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
26. Administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami nie posiadającymi zainstalowanego programu zabezpieczającego.
27. Agent musi przekazywać informacje na temat stanu systemu operacyjnego do Serwer administracyjna zarządzającego.
28. Agent musi posiadać możliwość pobrania listy

	zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania. 29. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie. 30. Instalacja agenta musi odbywać się przy wykorzystaniu repozytorium producenta. Repozytorium powinno zawierać aktualne wersje agentów bez względu na rodzaj systemu operacyjnego. 31. 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. 32. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika. 33. W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play. 34. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji. 35. 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. 36. Serwer administracyjny musi oferować możliwość utworzenia polityk konfiguracji dla aplikacji zabezpieczającej na urządzeniu mobilnym. 37. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi. 38. Administrator musi posiadać możliwość utworzenia użytkownika wbudowanego lub zintegrowanego z grupą z usługi Active Directory. 39. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp. 40. Administrator musi posiadać możliwość nadania

	dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis. 41. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika. 42. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta bez konieczności logowania się do panelu administracyjnego. 43. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany. 44. Dostępne zadania muszą być podzielone na dwie grupy: zadania klienta oraz zadania serwera. 45. Zadania serwera obejmujące zadanie instalacji agenta, generowania raportów oraz synchronizacji grup. 46. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej. 47. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji. 48. 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. 49. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym. 50. Serwer administracyjny musi oferować możliwość wyboru parametrów pakietu instalacyjnego zależnych od systemu operacyjnego oraz licencji na program zabezpieczający. 51. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu. 52. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką. 53. Serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy. 54. Serwer administracyjny musi oferować możliwość uruchomienia zadania automatycznie zgodnie z harmonogramem, po wystąpieniu nowego dziennika zdarzeń lub umieszczeniu nowego klienta w grupie

	dynamicznej. 55. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów. 56. 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. 57. Serwer administracyjny musi oferować możliwość utworzenia polityk dla programów zabezpieczających i modułów serwera centralnego zarządzania. 58. 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. 59. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej. 60. 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 względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku. 61. Serwer administracyjny musi oferować możliwość ukrycia graficznego interfejsu użytkownika na stacji klienckiej i jego uruchomienia tylko przez administratora. 62. Serwer administracyjny musi umożliwiać wyświetlenie polityk do których przynależy dana stacja robocza oraz ich edycję z poziomu właściwości samego klienta 63. Serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów. 64. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania. 65. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie. 66. Serwer administracyjny musi oferować możliwość wyboru jednego z kilku typów wykresów: kołowy,

	pierścieniowy, liniowy, słupkowy, punktowy, itp. 67. Serwer administracyjny musi oferować możliwość określenia danych jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na elementach wykresu oraz ich odfiltrowania i posortowania. 68. Serwer administracyjny musi być wyposażona w mechanizm importu oraz eksportu szablonów raportów. 69. Serwer administracyjny powinien posiadać Panel kontrolny z raportami administratora, pozwalający na szybki dostępu do najbardziej interesujących go danych. Panel ten musi oferować możliwość modyfikacji jego elementów. 70. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW. 71. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS. 72. Serwer administracyjny musi oferować możliwość skonfigurowania czasu automatycznego odświeżania raportu na panelu kontrolnym oraz umożliwiać jego odświeżenie na żądanie. 73. Serwer administracyjny musi oferować możliwość tworzenia wielu zakładek panelu, w których będą widoczne wybrane przez administratora elementy monitorujące. 74. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego. 75. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy. 76. Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień lub skorzystanie z predefiniowanych wzorów. 77. 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. 78. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP. 79. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w

	powiadomieniu. 80. Serwer administracyjny musi oferować możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu. 81. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta. 82. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji. 83. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty. 84. Serwer administracyjny musi oferować możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela. 85. Narzędzie administracyjne musi być wyposażone w mechanizm wyszukiwania zarządzanych komputerów na podstawie co najmniej nazwy komputera, adresu IPv4 i IPv6 lub wyszukania konkretnej nazwy zagrożenia. 86. Serwer administracyjny musi być wyposażona w machizm autodopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana. 87. Administrator musi mieć możliwość określenia zakresu czasu w jakim dane zadanie będzie wykonywane (sekundy, minuty, godziny, dni, tygodnie).

5.2. Komputer przenośny laptop wraz z oprogramowaniem systemowym i oprogramowaniem antywirusowym – 10 szt.

Komputer przenośny laptop – matryca 15” HD, procesor dwurdzeniowy czterowątkowy, 8GB DDR4, 500GB HDD, Grafika zintegrowana, system operacyjny w wersji PRO , 3 lat gwarancji

Specyfikacja dla sprzętu:

Nazwa komponentu	*Wymagane minimalne parametry techniczne*
Zastosowanie	Komputer przenośny będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji dziedzinowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna
Przekątna ekranu	Komputer przenośny typu notebook z ekranem 15,0" o rozdzielczości: HD (1366 x 768) z podświetleniem LED i powłoką

	przeciwodblaskową, jasność 200 nits, kontrast 300:1
Procesor	Procesor powinien osiągać w teście wydajności PassMark Performance Test co najmniej wynik 3950 punktów Passmark CPU Mark. Wynik dostępny na stronie: http://www.passmark.com/products/pt.htm
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.
Pamięć RAM	8GB (1x8GB) DDR4 SDRAM 2133MHz możliwość rozbudowy do min 16GB, wymagane min. 2 sloty na pamięci w tym min. jeden wolny
Pamięć masowa	SATA 500 GB 7200 RPM
Karta graficzna	Zintegrowana w procesorze z możliwością dynamicznego przydzielenia pamięci systemowej, Oferowana karta graficzna musi osiągać w teście PassMark Performance Test co najmniej wynik 740 punktów w G3D Rating, wynik dostępny na stronie: http://www.videocardbenchmark.net/gpu_list.php
Klawiatura	Klawiatura wyspowa z powłoka antybakteryjna, z wbudowanym w klawiaturze podświetleniem z możliwością manualnej regulacji zarówno w BIOS jak i z pod systemu operacyjnego, (układ US -QWERTY), min 80 klawiszy
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. Wbudowana kamera.
Bateria i zasilanie	Min. 4-cell [62Whr]. Umożliwiająca jej szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin. Czas pracy na baterii min 180 minut, potwierdzony przeprowadzonym testem MobileMark 2014 Battery Life [do oferty załączyć wydruk przeprowadzonego testu oraz dodatkowo w wersji elektronicznej pliki .pdf i .fdr w celu weryfikacji poprawności przeprowadzonego testu] Zasilacz o mocy min. 65W,
Obudowa	Szkielet obudowy i zawiasy notebooka wykonany z wzmacnianego metalu, dookoła matrycy gumowe uszczelnienie chroniące klawiaturę notebooka po zamknięciu przed kurzem i wilgocią. Kąt otwarcia notebooka min 180 stopni. Obudowa spełniająca normy MIL-STD-810G.

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 dla poszczególnych komponentów systemu).
BIOS	BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, wymagana pełna obsługa za pomocą klawiatury i myszy lub urządzenia wskazującego zintegrowanego (wmontowanego na stałe) w oferowanym urządzeniu Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: ▪ wersji BIOS, ▪ nr seryjnego komputera, ▪ 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 ▪ typie zainstalowanego procesora ▪ liczbie rdzeni procesora ▪ minimalnej prędkości zegara procesora ▪ maksymalnej prędkości zegara procesora ▪ wielkości pamięci podręcznej procesora L2 cache ▪ wielkości pamięci podręcznej procesora L3 cache ▪ technologii xx-bit procesora ▪ zainstalowanym i podpiętym HDD ▪ 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 ▪ zainstalowanym Bluetooth
Certyfikaty	Certyfikat ISO9001:2000 dla producenta sprzętu (należy załączyć do oferty). Certyfikat ISO 14001 dla producenta sprzętu (należy załączyć do oferty). Deklaracja zgodności CE (załączyć do oferty). Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji

	substancji niebezpiecznych w postaci oświadczenia producenta jednostki. Potwierdzenie kompatybilności komputera na stronie Windows Logo'd Products List na daną platformę systemową (wydruk ze strony). EnergyStar 6.0 – załączyć do oferty certyfikat.
Diagnostyka	Wbudowany system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot umożliwiający jednoczesne przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego.
Bezpieczeństwo	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 dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej. Czujnik spadania zintegrowany z płytą główną działający nawet przy wyłączonym notebooku oraz konstrukcja absorbująca wstrząsy. Czytnik linii papilarnych FIPS. Złącze typu Kensington Lock.
System operacyjny	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).
Dodatkowe oprogramowanie	Zainstalowane oprogramowanie z bezterminową licencją do wykonywania aktualizacji systemu i jego zasobów umożliwiające : - określenie preferencji aktualizacji - ustawienie priorytetu aktualizacji - użycia opcji planowania aktualizacji bieżących wersji sterowników. Dołączone do oferowanego komputera oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające : - 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 : a. o poprawkach i usprawnieniach dotyczących aktualizacji b. dacie wydania ostatniej aktualizacji c. priorytecie aktualizacji d. zgodność z systemami operacyjnymi e. jakiego komponentu sprzętu dotyczy aktualizacja f. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e. - 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 rozbiciem 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. Oprogramowanie producenta komputera z licencją bezterminową dedykowane dla zarządzania baterią, dostępne z poziomu system operacyjnego dla użytkownika oraz dla administratora z poziomu zdalnego zarządzania bez potrzeby konfigurowania ustawień w BIOS. Oprogramowanie musi umożliwiać co najmniej odczytanie Informacji o :

	- Żywotności baterii - % (procentowym) statusie naładowania baterii - Ustawionej opcji zarządzania baterią w BIOS'ie - Numerze seryjnym baterii Musi umożliwiać ustawienie zaawansowanego planu ładowania baterii w zakresie: - poszczególny dzień tygodnia (określenie do godziny i minuty czasu ładowania) - zdefiniowanie harmonogramu tylko dla jednego dnia i powielenia go dla pozostałych - możliwość ustawienia zakresu czasowego pracy tylko na samej baterii nawet kiedy jest podpięte zasilanie - możliwość ustawienia zakresu czasowego pracy tylko na zasilaniu sieciowym mimo naładowania baterii w 100%, bez włączania ładowania i doładowywania, - możliwość ustawienia zakresu czasowego pracy tylko na zasilaniu sieciowym wraz z jednoczesnym ładowaniem baterii. Musi posiadać Możliwość ustawienia automatycznego przywrócenia zasilania sieciowego w przypadku osiągnięcia krytycznej % wydajności baterii określonej przez administratora bądź użytkownika. Zarządzanie termiczne odpowiedzialne za wydajność procesora, głośność pracy wentylatora oraz kontrolowanie za pomocą czujnika termicznego wewnętrznej temperatury możliwość ustawienia opcji w minimum czterech wariantach (np. zrównoważony, chłodzenie, cichy bądź wydajny) zdefiniowanych przez oprogramowanie.
Porty i złącza	Wbudowane porty i złącza : - 1x VGA - 1x HDMI - 1x RJ-45 (10/100/1000) - 2x USB 3.0 - 1x USB 3.0 dosilony, przeznaczony min. do obsługi bez dodatkowego zasilania zewnętrznych HDD - czytnik kart multimedialny wspierający karty SD 4.0 - czytnik kart SmartCard - czytnik linii papilarnych - współdzielone złącze słuchawkowe stereo i złącze mikrofonowe tzw. combo - Dedykowany port umożliwiający podłączenie dedykowanej stacji dokującej [nie dopuszcza się stosowania rozwiązania tzw. replikator portów podłączany przez port USB] - port zasilania - moduł bluetooth 4.0 dopuszcza się współdzielony z kartą WiFi

	- touchpad z strefą przewijania w pionie, poziomie wraz z obsługą gestów - Zintegrowana w postaci wewnętrznego modułu mini-PCI Express karta sieci WLAN obsługująca łącznie standardy IEEE 802.11 AC
Gwarancja	5-letnia gwarancja producenta świadczona na miejscu u klienta, Czas reakcji serwisu - do końca następnego dnia roboczego. Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty.
Oprogramowanie antywirusowe	Zainstalowane oprogramowanie antywirusowe opisane w punkcie 5.1.

5.3. Oprogramowanie biurowe – 10 szt.

Pakiet oprogramowania biurowego zawierającego następujące komponenty:
- edytor tekstów,
- arkusz kalkulacyjny,
- narzędzie do przygotowania i prowadzenia prezentacji,
- narzędzie do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami).

Specyfikacja:

Nazwa komponentu	*Wymagane minimalne parametry techniczne*
Zastosowanie	Zintegrowany pakiet aplikacji biurowych, w którego skład ma wchodzić min.: - edytor tekstów; - arkusz kalkulacyjny; - narzędzie do przygotowania i prowadzenia prezentacji; - narzędzie do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami); - 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 w dni robocze w godzinach od 8-19 – cena połączenia nie większa niż cena połączenia lokalnego - publicznie znany cykl życia przedstawiony przez producenta dotyczący rozwoju i wsparcia technicznego – w szczególności w zakresie bezpieczeństwa co najmniej 3 lata 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 prezentowanie 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 (pocztą 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, - - 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 przesyłania kontaktów innym użytkowników.

5.4. Tablet wraz z oprogramowaniem systemowym i oprogramowaniem antywirusowym – 5 szt.

Tablet z odłączaną klawiaturą – matryca 12" IPS 2160x1440, procesor dwurdzeniowy, 4GB DDR3, 128GB SSD, Grafika zintegrowana, WiFi 802.11 ac, system operacyjny w wersji PRO, 3 lat gwarancji.

Specyfikacja dla sprzętu:

Nazwa komponentu	*Wymagane minimalne parametry techniczne*
Zastosowanie	Komputer przenośny będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji dziedzinowych, dostępu do Internetu oraz poczty elektronicznej.
Przekątna ekranu	Tablet 12,0" IPS o rozdzielczości 2160x1440, typ ekrany pojemnościowy, 10-punktowy
Procesor	Procesor powinien osiągać w teście wydajności PassMark Performance Test co najmniej wynik 3190 punktów Passmark CPU Mark. Wynik dostępny na stronie: http://www.passmark.com/products/pt.htm
Pamięć RAM	4GB DDR3
Pamięć masowa	128 GB SSD
Karta graficzna	Zintegrowana w procesorze z możliwością dynamicznego przydzielenia pamięci systemowej, Oferowana karta graficzna musi osiągać w teście PassMark Performance Test co najmniej wynik 560 punktów w G3D Rating, wynik dostępny na stronie: http://www.videocardbenchmark.net/gpu_list.php
Klawiatura	Klawiatura odłączalna za pomocą funkcjonalnego zawiasu, który umożliwia szybkie łączenie i rozłączanie ekranu i klawiatury z touchpadem.
Multimedia	Wbudowany głośnik i mikrofon. Wbudowana kamery 5.0 Mpix (przód 5 Mpix - tył 5 Mpix)
Bateria i zasilanie	Min. 4-cell Typ zasilania akumulator litowo-polimerowy Żywotność baterii 9 h
Złącza	Czytnik kart pamięci - 1 szt. DC-in (wejście zasilania) - 1 szt. Wyjście słuchawkowe - 1 szt. Micro HDMI - 1 szt. USB 3.0 - 1 szt.

Łączność	Moduł Bluetooth Wi-Fi 802.11 ac
Gwarancja	5-letnia gwarancja producenta świadczona na miejscu u klienta, Czas reakcji serwisu - do końca następnego dnia roboczego.
System operacyjny	Zainstalowany system operacyjny w wersji Professional
Oprogramowanie antywirusowe	Zainstalowane oprogramowanie antywirusowe opisane w punkcie 5.1.

5.5. Drukarka laserowa mono – 45 szt.

Drukarka laserowa mono – prędkość druku do 38 str/min. Rozdzielczość druku 1200x1200, 3 lat gwarancji

Specyfikacja dla sprzętu:

Nazwa komponentu	*Wymagane minimalne parametry techniczne*
Funkcje	Drukowanie mono
Pamięć standardowa/ maksymalna	128 MB / 512 MB
Interfejsy	Ethernet 10 / 100 Base TX / High Speed USB 2.0
Maks. miesięczny cykl obciążenia	80 000 stron
Szybkość (druk czarno-biały)	Min. 38 str/min A4
Rozdzielczość	Min. 1 200 x 1 200 dpi rozdzielczości efektywnej
Emulacja	PostScript3 / PCL6 / PCL5e
Drukowanie dwustronne	Tak
Kaseta	Podajnik kasetowy standardowy na 250 arkuszy - 60 – 163 g/m² Uniwersalny podajnik na 50 arkuszy - 60 – 220 g/m²
Pojemność odbiornika	Min. 150 arkuszy drukiem do dołu, 1 arkusz drukiem do góry
Panel operacyjny	Dwuwierszowy wyświetlacz LCD, klawiatura numeryczna
Poziom hałasu	Drukowanie poniżej 54 dBA / tryb czuwania poniżej 26 dBA
Gwarancja	5-letnia gwarancja producenta

5.6. Drukarka laserowa kolorowa – 3 szt.

Drukarka laserowa kolorowa – prędkość druku do 24 str/min. Rozdzielczość druku 1200x600, 3 lata gwarancji.

Specyfikacja dla sprzętu:

Nazwa komponentu	*Wymagane minimalne parametry techniczne*
Funkcje	Drukowanie mono i kolor
Pamięć standardowa/ maksymalna	256 MB / 512 MB
Interfejsy	Hi-Speed USB 2.0, Host USB, Ethernet 10 / 100 / 1000 Base-TX
Maks. miesięczny cykl obciążenia	60 000 stron

Szybkość druk czarno-biały i kolor	Min. 24 str/min A4 mono i kolor
Rozdzielczość	Min. Do 9 600 x 600 dpi rozdzielczości efektywnej
Emulacja	PCL5Ce / PCL6C / PS3 / PDF V1.7
Drukowanie dwustronne	Tak
Kaseta	Standardowa kaseta na 250 arkuszy Podajnik wielozadaniowy na 50 arkuszy
Pojemność odbiornika	Min. 150 arkuszy drukiem do dołu
Panel operacyjny	Dwuwierszowy wyświetlacz LCD
Poziom hałasu	Drukowanie poniżej 52 dBA / tryb czuwania poniżej 32 dBA
Gwarancja	5-letnia gwarancja producenta

5.7. Urządzenie wielofunkcyjne mono - 6 szt.

Urządzenie wielofunkcyjne kolorowe – prędkość druku do 24 str/min. Rozdzielczość druku 1200x600, 3 lata gwarancji

Specyfikacja dla sprzętu:

Nazwa komponentu	*Wymagane minimalne parametry techniczne*
Funkcje	Drukowanie / kopiowanie / skanowanie / faksowanie/ e-mail
Pamięć standardowa/ maksymalna	512 MB / 1024 MB
Interfejsy	Hi-Speed USB 2.0, host USB, Ethernet 10 / 1 000 Base-TX, IEEE 802.11b/g/n Wireless Network
Maks. miesięczny cykl obciążenia	60 000 stron
Szybkość druk czarno-biały	Min. 24 str/min A4
Rozdzielczość drukowania	Min. Do 9 600 x 600 dpi rozdzielczości efektywnej
Drukowanie dwustronne	Tak
Emulacja	PCL5Ce / PCL6C / PS3 / PDF V1.7
Kopiowanie - rozdzielczość	Optyczna: Do 600 x 600 dpi
Kopiowanie - powiększenie	25–400% (podajnik automatyczny, szyba)
Kopiowanie wielokrotne	1-999 stron
Funkcje kopiowania	Kopiowanie dokumentów, kopiowanie kilku stron na jednym arkuszu, kopiowanie książek, kopiowanie ze znakiem wodnym, kopiowanie scalone
Skanowanie - metoda	Kolor CIS
Skanowanie kompatybilność	Standard Twain / standard WIA
Skanowanie rozdzielczość	Min. Optyczna rozdzielczość 1 200 x 1 200 dpi
Funkcje skanowania	USB / e-mail / SMB / FTP / PC

Format papieru skan i druk	Min. A3 i A4
Faks kompatybilność	ITU-T G3
Pamięć faxu	6 MB
Funkcje faksu	Multiwysyłka / Odroczona wysyłka / Zabezpieczenie odbioru / Przekazywanie faksu
Kaseta	Standardowa kaseta na 250 arkuszy Podajnik wielozadaniowy na 50 arkuszy
Pojemność odbiornika	Min. 150 arkuszy drukiem do dołu
Panel operacyjny	Ekran dotykowy LCD 4,3", jednoprzyciskowy tryb eko, bezpośredni port USB, funkcja drukowania z urządzeń przenośnych
Poziom hałasu	Drukowanie poniżej 52 dBA / kopiowanie poniżej 54 dBA / Tryb gotowości poniżej 32 dBA
Gwarancja	3-letnia gwarancja producenta

5.8. Skaner dokumentowy – 6 szt.

Skaner dokumentowy – prędkość druku do 24 str/min. Rozdzielczość druku 1200x600, 3 lata gwarancji

Specyfikacja istotnych warunków zamówienia dla sprzętu:

Nazwa komponentu	*Wymagane minimalne parametry techniczne*
Rodzaj lampy	LED
Czas nagrzewania	poniżej 1 sekundy
Szybkość skanowania	A4 mono/kolor (300dpi): 30 str./min., 60 obr./min. przy 300 dpi
Podajnik	50 arkuszy A4 (80 g/m2)
Rozdz. optyczna w pionie	600 dpi
Rozdz. optyczna w poziomie	600 dpi
Wewnętrzna głębia koloru	48 bit
Zewnętrzna głębia koloru	24 bit
Przyciski funkcyjne	Tak
Czujnik ultradźwiękowy	Tak
Maks. szerokość skanowania	216 mm
Maks. długość skanowania	900 mm
Obsługiwana gramatura	50 - 400 g/m²
Interfejs	USB 2.0
Dodatkowe informacje	skanowanie dwustronne jednoprzebiegowe
Dzienna wydajność niezawodnej pracy	3 000 str.
Wydajność rolek	min. 100.000 skanów

Sterowniki	TWAIN, WIA, ISIS, Windows Server 2003/2008/2012, Linux (debian, opensuse, ubuntu, fedora)
Funkcje skanera	Możliwość rozbudowy skanera o oryginalny panel/kartę sieciową producenta 10/100/1000 Mbit
	Możliwość tworzenia profili, ich eksportowania oraz importowania do innych skanerów w grupie roboczej
	Tworzenie dokumentów PDF z funkcją przeszukiwania w j. polskim
	Możliwość tworzenia automatycznego raportu skanowania po każdym zadaniu w osobnym pliku formatu CSV lub XML
	Bezpośrednie skanowanie do Microsoft SharePoint Server, WebDav, SugarSync, Evernote oraz Google Drive
	Separacja zadań po kodzie kreskowym
	Automatyczne tworzenie plików o nazwie będącej informacją zawartą w kodzie kreskowym
	Usuwanie otworów po dziurkaczu
	Automatyczna korekta położenia ukośnego
	Automatyczny obrót obrazu
	Separacja kolorów
	Automatyczne łączenie dwóch skanów A4 do formatu A3
Gwarancja	3-letnia gwarancja producenta

5.9. Drukarka opasek – 3 szt.

Drukarka opasek dla pacjenta – rodzaj druku – termiczny, prędkość druku do 51 mm/s. Max. szerokość druku: 19 mm, 25 mm, 30 mm, 3 lata gwarancji.

Specyfikacja istotnych warunków zamówienia dla sprzętu:

Nazwa komponentu	*Wymagane minimalne parametry techniczne*
Rodzaj druku	termiczny
Rozdzielczość	300 dpi
Prędkość druku	51 mm/s
Max. szerokość druku	19 mm, 25 mm, 30 mm
Max długość druku	558 mm
Waga	Do 1,5 kg
Rodzaj obudowy	plastikowa
Temperatura pracy	4,4-40ºC
Pamięć	16 MB SDRAM, 8 MB Flash
Interfejs	RS232, USB
Zasilacz	100-240 V/50-60Hz
Język programowania	XML, ZPL, ZPL I/ZPL II, ZPL II
Drukowane kody kreskowe	LINIOWE Code 11, Code 39, Code 93, Code 128, UPC-A, UPC-E, EAN-8, EAN-13, EAN-14, UPC-A and UPC-E with EAN 2 or 5 digit extensions, Plessey, POSTNET, Standard 2 of 5, Industrial 2 of 5, Interleaved 2 of 5, LOGMARS, MSI, Codabar, and GS1 DataBar (formerly RSS)DWUWYMIAROWE PDF417, MicroPDF-417, Code 49,

	Maxicode, Codablock, Data Matrix, QR code, Aztec
Oprogramowanie	Przynajmniej: sterownik drukarki Windows,
Gwarancja	Rok, gwarancja producenta

6. Uwagi końcowe

Urządzenia i osprzęt wyspecyfikowany w zestawieniu materiałów należy traktować jako przykładowy i może zostać zamieniony na inny pod warunkiem, że dostawca przedstawi dokumenty, że aparatura zamienna ma te same lub lepsze parametry techniczne od zaproponowanej, taką sama barwę i okres gwarancji.

Przy przewidywaniu zastosowania aparatury równorzędnej należy przedstawić Inwestorowi karty katalogowe proponowanej aparatury.

Podczas wykonywania prac instalacyjno-montażowych należy zwracać szczególną uwagę na istniejące instalacje natynkowe i podtynkowe tj. instalacje alarmowe, telefoniczne, wodno-kanalizacyjne oraz zasilania elektrycznego. W przypadku jakichkolwiek wątpliwości lub problemów należy konsultować się z właściwymi służbami technicznymi Szpitala.

Wykonawca musi zapewnić autoryzowane certyfikowane szkolenie w następujących obszarach

obszar	*poziom*	*Liczba osób*
System operacyjny	Podstawowy administracja	1
System operacyjny	zaawansowany administracja	1
Baza/y danych	Podstawowy administracja	1
Wirtualizacja	Podstawowy administracja	1
Usługi katalogowe	Podstawowy administracja	1