Załącznik nr 9 do SIWZ

INNOWACYJNA GOSPODARKA
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ
ROZWOJU REGIONALNEGO

Inwestor: **Gmina Prusice**

ul. Rynek 1

55-110 Prusice

Temat opracowania:

PROGRAM FUNKCJONALNO – UŻYTKOWY

DLA PROJEKTU :

„Informatyzacja Gminy Prusice jako sposób na przeciwdziałanie wykluczeniu cyfrowemu”. realizowanego przez Gminę Prusice w ramach „ Działania 8.3. Programu Operacyjnego Innowacyjna Gospodarka na lata 2007-2013”

Data opracowania :	Październik 2013
Podpis osoby upoważnionej do reprezentowania Zamawiającego :	

Kod zamówienia

1. Usługi inżynieryjne z zakresie projektowania Kod CPV 71320000-7
2. Wznoszenie masztów antenowych Kod CPV 45232330-4
3. Wieże , maszty kratowe , półmaszty i słupy stalowe Kod CPV 44212200-1
4. Sieć radiowa Kod CPV 32418000-6
5. Sprzęt do przesyłu danych Kod CPV 32581000-9
6. Serwery sieciowe Kod CPV 48821000-9
7. Routery sieciowe Kod CPV 32413100-2
8. Sieć internetowa Kod CPV 32412110-8
9. Urządzenia sieciowe Kod CPV 32420000-3

10. Awaryjne urządzenia energetyczne Kod CPV 31682530-4
11. Instalowanie urządzeń telekomunikacyjnych Kod CPV 45314000-1
12. Montaż anten radiowych Kod CPV 45312330-9
13. Telekomunikacyjne roboty dodatkowe Kod CPV 45232332-8
14. Instalowanie urządzeń klimatyzacyjnych Kod CPV 45331220-4
15. Roboty instalacyjne elektryczne Kod CPV 45310000-3
16. Roboty wykończeniowe w zakresie obiektów budowlanych Kod CPV 45400000-1
17. Instalowanie okablowania komputerowego Kod CPV 45314320-0

18. Urządzenia komputerowe Kod CPV 30230000-0
19. Instalacja wyposażenia Kod CPV 45421153-1
20. Usługi w zakresie napraw i konserwacji i podobne usługi dotyczące komputerów osobistych, sprzętu biurowego, sprzętu telekomunikacyjnego Kod CPV 50300000-8

21. Usługi w zakresie rozległej sieci komputerowej Kod CPV 72720000-3
22 Usługi w zakresie wsparcia technicznego Kod CPV 72611000-6

.

Zawartość

I. Część opisowa programu

II. Ogólne wymagania zamawiającego

III. Aktualne uwarunkowania przedmiotu zamówienia

IV. Ogólne właściwości funkcjonalno-użytkowe

V. Szczegółowe właściwości i wymagania funkcjonalno-użytkowe

1. W zakresie dokumentacji projektowej
2. W zakresie budowy wież /masztów antenowych oraz konstrukcji wsporczych pod anteny
3. W zakresie budowy sieci szkieletowej i dystrybucyjnej
4. W zakresie budowy węzłów dostępowych
5. W zakresie budowy Głównego Węzła Dystrybucyjnego i Centrum Zarządzania siecią
6. W zakresie dostawy i instalacji sprzętu komputerowego i oprogramowania dla 80 gospodarstw domowych objętych projektem.
7. W zakresie serwisu ,utrzymania wybudowanej infrastruktury i urządzeń.

VI. Ogólne warunki wykonania i odbioru robót

VII. Część informacyjna programu

1. Akty prawne i rozporządzenia

I. Cześć opisowa programu funkcjonalno-użytkowego

1.1.Opis ogólny przedmiotu zamówienia

Przedmiot zamówienia w ramach realizacji projektu pt. „**Informatyzacja Gminy Prusice jako sposób na przeciwdziałanie wykluczeniu cyfrowemu"** należy wykonać w modelu zaprojektuj i wybuduj.

Głównym celem projektu jest przeciwdziałanie zjawisku wykluczenia cyfrowego, jakie występuje, lub może występować, wśród mieszkańców Gminy Prusice . Przeprowadzony audyt infrastruktury posiadanej przez Gminę, infrastruktury internetowej oraz zasięgu i jakości usług działających na tym terenie operatorów telekomunikacyjnych oraz ISP wykazał, że niezbędna jest budowa własnej infrastruktury telekomunikacyjnej. Dodatkowo stwierdzono, że rozmieszczenie Beneficjentów Ostatecznych (ozn. dalej BO) jest stosunkowo równomierne na całym obszarze projektu, jak również fakt, że alokacja BO w czasie trwania projektu jak i w okresie trwałości jest również dopuszczalna. Te czynniki wymuszają przyjęcie n/w założeń funkcjonalno-ekonomicznych. Gmina Prusice zamierza wybudowaną infrastrukturę wykorzystać w przyszłości do poszerzenia projektu o kolejne grupy wykluczonych , bez ponoszenia większych nakładów na jej rozbudowę.

Stąd też założono, że jedynie radiowa sieć szerokopasmowa oparta na odpowiedniej ilości węzłów dostępowych, obejmująca zasięgiem min. 90% obszaru projektowego (zamieszkałego) tak postawione cele może spełnić.

W wyniku realizacji zamówienia przez Wykonawcę zostanie wybudowana infrastruktura umożliwiająca dostęp do Internetu oraz zostaną zakupione zostaną zestawy komputerowe dla beneficjentów ostatecznych biorących udział w projekcie.

Zostanie wykonana sieć telekomunikacyjna o strukturze hierarchicznej, składająca się z trzech podstawowych poziomów:

- sieci szkieletowej

- sieci dystrybucyjnej

- sieci dostępowej

1.2 Ogólny zakres zamówienia :

1. Zaprojektowanie i wybudowanie wież/masztów oraz innych niezbędnych konstrukcji wsporczych.
2. Adaptację pomieszczenia na serwerownię wraz instalacją niezbędnych urządzeń sieciowych (Głównego Węzła Dystrybucyjnego i Centrum Zarządzania Siecią)
3. Wykonanie połączeń i węzłów szkieletowych.
4. Wykonanie połączeń i węzłów dystrybucyjnych.
5. Wykonanie węzłów dostępowych które stanowić będą podstawową infrastrukturę teleinformatyczną zapewniającą dostęp do Internetu dla uczestników projektu .
6. Zakup i instalację zestawów komputerowych oraz radiowych jednostek abonenckich dla uczestników projektu (BO)

1.3 Szczegółowy zakres robót , dostaw i usług

1. **Przygotowania dokumentacji projektowej, harmonogramu prac oraz innej niezbędnej dokumentacji**
   - Opracowanie koncepcji technicznej sieci
   - Opracowanie projektów budowlanych w zakresie budowy wież / masztów antenowych (wraz z branżami), oraz niezbędną dokumentacją związaną z uzyskaniem pozwolenia na budowę (jeśli będzie wymagane)
   - Opracowanie projektu wykonawczego budowy sieci szerokopasmowej
   - Opracowanie szczegółowego harmonogramu prac

2. **Budowy wież , masztów antenowych i innych konstrukcji wsporczych**
   - Budowa wież / masztów antenowych w miejscowościach gminy Prusice w ilości wynikających z projektu , zapewniających wymagane pokrycie sygnałem.
   - Instalacja szaf zewnętrznych lub wewnętrznych, w zależności od projektu oraz wykonanie instalacji okablowania sygnałowego i zasilającego pod potrzeby instalacji urządzeń radiowych i sieciowych

3. **Budowy sieci szkieletowej oraz dystrybucyjnej**
   - Dostawa, instalacja oraz konfiguracja radiolinii cyfrowych
   - Dostawa, instalacja oraz konfiguracja połączeń punkt-punkt

4. **Budowy sieci dostępowej (Węzłów Dostępowych oraz instalacja terminali odbiorczych)**
   - Dostawa, instalacja i konfiguracja elementów oraz urządzeń stanowiących wyposażenie węzłów dostępowych
   - Dostawa, instalacja i konfiguracja przełączników sieciowych oraz UPS-ów
   - Montaż szaf, wsporników antenowych oraz przygotowanie infrastruktury kablowej w obiektach węzłów dostępowych
   - Dostawa i instalacja i konfiguracja urządzeń odbiorczych dla 80 BO

5. **Wyposażenia Głównego węzła dystrybucyjnego i Centrum zarządzania siecią**

- Wykonanie adaptacji pomieszczenia w wybranej lokalizacji
- Modernizacja sieci elektrycznej w pomieszczeniu.
- Zakup i montaż drzwi antywłamaniowych.
- Zakup i instalacja klimatyzacji.
- Montaż podłogi technicznej
- Zakup, instalacja i konfiguracja urządzeń i osprzętu niezbędnych do prawidłowego funkcjonowania Centrum zarządzania siecią (przełącznika szkieletowego, kontrolera sieci bezprzewodowej, urządzenia bezpieczeństwa, serwerów oraz implementacja systemów do zarządzania użytkownikami i usługami sieci opisanych w dalszej części PFU)

6. **Dostarczenie i instalację zestawów komputerowych oraz oprogramowania do BO.**
- Dostawa i instalacja 80 zestawów komputerowych z oprogramowaniem oraz podłączenie ich do radiowych terminali odbiorczych w wybranych przez Zamawiającego 80 uczestników projektu znajdujących się na terenie objętym projektem w Gminie Prusice.

7. **Przeprowadzenie wymaganych prób i badań funkcjonowania infrastruktury oraz przygotowanie dokumentów związanych z odbiorem przedmiotu zamówienia i rozpoczęciem eksploatacji sieci internetowej .**
- Przeprowadzenie konfiguracji sieci, sprawdzenia jej funkcjonowania u każdego z użytkowników końcowych.
- Przeprowadzenie testów dla urządzeń transmisyjnych warstwy szkieletowej i dystrybucyjnej
- Przeprowadzenie demonstracji działania systemy monitoringu i zarządzanie siecią i użytkownikami zainstalowanymi w GWD i CZS

- Przygotowanie protokołu odbioru wykonanych w ramach realizacji projektu robót
- Przygotowanie dokumentacji powykonawczej
- Przeprowadzenie szkolenie dla administratorów sieci ze strony Zamawiającego

8. Usługi utrzymania i serwisu infrastruktury sieciowej i urządzeń komputerowych.

- Serwis i utrzymywanie sprzętu komputerowego u BO (80 zestawów komputerowych z dostępem do wybudowanej sieci) wraz z wsparciem technicznym
- Serwis i utrzymanie wybudowanej infrastruktury sieci szerokopasmowej.

II . OGÓLNE WYMAGANIA ZAMAWIAJĄCEGO

Program funkcjonalno-użytkowy określa wymagania dotyczące zaprojektowania, realizacji i przekazania w użytkowanie wszystkich elementów opisywanego systemu. Wykonawca podejmujący się realizacji przedmiotu zamówienia zobowiązany jest do:
- dokonania wizji w terenie, celem szczegółowego zapoznania się z zakresem prac oraz uwarunkowaniami terenowymi,
- opracowania dokumentacji projektowej zgodnie z umową, przepisami techniczno-budowlanymi, wymaganiami określonymi w programie funkcjonalno-użytkowym , normami i wytycznymi w tym zakresie,
- opracowania i przedstawienia zamawiającemu do zatwierdzenia szczegółowego harmonogramu prac,
- wykonania i odbioru robót budowlanych określonymi w programie funkcjonalno-użytkowym, powszechnie obowiązującymi przepisami prawa i normami budowlanymi
- sporządzenie dokumentacji technicznej powykonawczej

Realizacja powyższego zakresu zamówienia powinna być wykonana w oparciu o obowiązujące przepisy, przez Wykonawcę posiadającego stosowne doświadczenie, uprawnienia i potencjał wykonawczy oraz osoby o odpowiednich kwalifikacjach i doświadczeniu zawodowym.

2.1 W zakresie usług i dostępności sieci

Zamawiający oczekuje, iż zrealizowany i uruchomiony system spełni następujące wymagania jakościowe i funkcjonalne:

- Szybkość łącza do BO min.: 6 Mb/s z możliwością zwiększenia do 18Mb/s
- Szybkość łącza od BO min.: 2 Mb/s z możliwością zwiększenia do 6 Mb/s
- Szybkość połączeń szkieletowych : symetrycznie , min. 200 Mb/s
- Szybkość połączeń dystrybucyjnych : symetrycznie ,min. 100 Mb/s
- Zapewnienie dostępności sieci na poziomie min. 99,98% (warstwa dystrybucyjna)
- Zapewnienie dostępności sieci na poziomie min. 99,99% (warstwa szkieletowa)
- Zapewnienie czasu usunięcia uszkodzenia 95% przypadków zgłoszonych usterek w czasie poniżej 48h
- Możliwość ustawienia strony www uruchamianej po zalogowaniu do systemu
- Możliwość blokowania wybranych stron www
- Możliwość blokady wybranych portów i usług (np. usług wymiany plików)

2.2 W zakresie technologii sieci bezprzewodowej

Zrealizowany i uruchomiony dostęp do Internetu z wykorzystaniem sieci bezprzewodowej powinien spełnić następujące wymagania:

- sieć w warstwie dostępowej oparta ma być na technologii 802.11 a/b/g/n (obsługa MIMO min. 2x2) i działać na uwolnionych przez Urząd Komunikacji Elektronicznej częstotliwościach 2,4 Ghz oraz 5,4-5,7 GHz, z zachowaniem obowiązujących przepisów w tym zakresie, w szczególności maksymalnej mocy e,i.r.p.
- wymaga się aby pojedyncze urządzenie punktu dostępowego (AP) posiadało 2 interfejsy radiowe tzw. Dual Band, każdy na inne pasmo uwolnione i bezpłatne w użytkowaniu
- wymaga się aby sieć dostępowa była obsługiwana przez kontroler WiFi
- sieć radiowa w warstwie dystrybucyjnej powinna być wykonana i funkcjonować w oparciu o licencjonowane pasmo niezbędne do zapewnienia jakości i pewności połączeń . W uzasadnionych przypadkach dopuszcza się możliwość pracy w oparciu o nielicencjonowane pasmo 5,4 - 5,7 GHz
- sieć radiowa w warstwie szkieletowej powinna być wykonana i funkcjonować tylko i wyłącznie w oparciu o licencjonowane pasmo niezbędne do zapewnienia jakości i pewności połączeń
- węzły dostępowe i dystrybucyjne powinny być wybudowane w pierwszej kolejności na obiektach należących do Gminy Prusice .
- jeden punkt dostępowy powinien zapewnić podłączenie co najmniej 5 użytkowników
- sieć powinna posiadać wsparcie dla najnowszych technologii bezpieczeństwa w zakresie autentykacji i autoryzacji użytkowników oraz bezpieczeństwa transmisji danych
- sieć powinna posiadać wsparcie dla usług QoS we wszystkich warstwach

Główny węzeł dystrybucyjny oraz Centrum zarządzania siecią powinien być zlokalizowany w obiekcie należącym do Zamawiającego i zawierać następujące systemy:
- zarządzania użytkownikami i usługami sieci
- zarządzania uszkodzeniami
- zarządzania konfiguracją
- zarządzania wydajnością
- zarządzania bezpieczeństwem
- monitoringu sieci
- autentykację użytkowników
- logowanie zdarzeń

2.3 . Ogólne wymagania obsługi gwarancyjno-serwisowej

- Wszystkie elementy wchodzące w skład przedmiotu zamówienia powinny być objęte 36 miesięczną gwarancją (o ile szczegółowe zapisy PFU nie stanowią inaczej)
- W okresie gwarancji Wykonawca zobowiązany jest zapewnić Zamawiającemu:
    - usuwanie wszelkich wad i nieprawidłowości powstałych na wskutek standardowej i zgodnej z przeznaczeniem eksploatacji przedmiotu zamówienia
    - przyjmowanie zgłoszeń serwisowych w godzinach 8.00-20.00 (telefonicznie pod wskazanym przez wykonawcę numerem telefonu) z możliwością zgłaszania awarii bezpośrednio u producenta (na wypadek braku reakcji serwisowej ze strony Wykonawcy)
    - dostęp do bezpośredniego wsparcia technicznego producenta

- W trakcie trwania gwarancji Wykonawca jest zobowiązany do wykonywania płatnych okresowych przeglądów gwarancyjnych.

Szczegółowe warunki w tym zakresie zostały opisane w pkt. 5.7.

Niniejszy Program Funkcjonalno-Użytkowy zawiera tylko podstawowe i minimalne wymagania funkcjonalne i techniczne w zakresie elementów i rozwiązań przeznaczonych do realizacji projektu. **Wykonawca może zaoferować sprzęt i rozwiązania dowolnego producenta, które spełniają wymagania określone w niniejszym dokumencie.**

Jeżeli w opisie przedmiotu zamówienia znajdują się jakiekolwiek znaki towarowe, patent, czy pochodzenie – należy przyjąć, że Zamawiający podał taki opis ze wskazaniem na typ i dopuszcza składanie ofert równoważnych o parametrach techniczno-eksploatacyjno-użytkowych nie gorszych niż te, podane w opisie przedmiotu zamówienia.

Wykonawca, który powołuje się na rozwiązania równoważne opisywane przez Zamawiającego jest obowiązany wykazać, że oferowane przez niego dostawy, usługi lub roboty budowlane spełniają wymagania określone przez Zamawiającego".

III. Aktualne uwarunkowania wykonania przedmiotu zamówienia.

Opis stanu istniejącego.

Gmina Prusice dysponuje nieruchomościami, na których mogą zostać wybudowane wieże lub maszty będące podstawą infrastruktury telekomunikacyjnej zapewniającej dostęp do Internetu. Są to nieruchomości gruntowe, budynki jednostek podległych oraz inne obiekty będące w dysponowaniu Gminy Prusice .

- Wykonawca w pierwszej kolejności będzie projektował konstrukcje na nieruchomościach należących do Gminy Prusice lub będącym w jej dysponowaniu.
- W następnym kroku, przy ich braku należy wykonać akwizycje innych nieruchomości gruntowych lub obiektów wysokościowych oraz uzyskać akceptację Inwestora.
- Zamawiający wymaga w pierwszej kolejności projektowania i wykonania konstrukcji stalowych lub Strunobetonowych wolnostojących (wieże) lub masztów stalowych z odciągami posadowionych na gruncie.

Uzyskanie wszelkich zgód i pozwoleń związanych z lokalizacją infrastruktury na gruncie /obiektach/budynkach właścicieli prywatnych, leży po stronie Wykonawcy.

Ewentualne koszty związane z dzierżawą, kolokacją i utrzymaniem infrastruktury na budynkach/obiektach nie należących do Zamawiającego muszą zostać przez niego zaakceptowane .

Gmina Prusice dysponuje pomieszczeniem na serwerownię (Głównego Węzła Dystrybucyjnego i Centrum Zarządzania Siecią) zlokalizowanym na 1 piętrze budynku UMiG w Prusicach. Zamawiający informuje , że budynek UMiG jest objęty ochroną konserwatorską . Wybrane przez Wykonawcę pomieszczenie zostanie udostępnione w celu jego adaptacji oraz wyposażenia przez Wykonawcę.

Wykonawca może zaproponować inną lokalizację serwerowni, która będzie wynikać z przedstawionego projektu technicznego sieci, spełniającą warunki postawione przez Zamawiającego.

Wykonawca projektując sieć musi brać pod uwagę aktualne warunki techniczne wykorzystania częstotliwości uwolnionych (2,4 i 5GHz) , w szczególności działających na jej obszarze lub w okolicy dostawców internetowych. Zamawiający oczekuje bowiem takich rozwiązań w zakresie doboru technologii radiowej, które zapewnią jakość i dostępność usług na poziomie określonym w niniejszym dokumencie przez okres minimum 6 lat. Zamawiający będzie miał prawo do powołania ekspertów zew. w celu zaopiniowania rozwiązań technicznych zaproponowanych przez Wykonawcę względem zapisów PFU.

IV. Ogólne właściwości funkcjonalno-użytkowe.

1) Liczba węzłów dostępowych i wynikająca stąd liczba sektorów radiowych ma być dobrana zależnie od warunków terenowych, obsługiwanej liczby odbiorców co powinno być poparte wynikami planowania radiowego.

2) Sieć dostępowa powinna objąć zasięgiem co najmniej 90% obszaru projektowego ,zamieszkałego co powinno być poparte wynikami planowania radiowego.

3) Sieć radiowa musi być tak zaprojektowana aby każde z połączeń szkieletowych i dystrybucyjnych posiadało odpowiednio zbilansowaną przepływność wynikającą z obciążeń (UL / DL) niezależnie od topologii jej wykonania.

4) W projekcie założono, że we wskazanym przez Gminę Prusice, lokalu Beneficjenta ostatecznego będzie instalowany radiowy terminal klienta typu zewnętrznego, który będzie bezpośrednio podłączony do zestawu komputerowego.

5) Adaptacja pomieszczenia na serwerownię polegać będzie na: zainstalowaniu klimatyzacji oraz systemu dostępu, modernizacji sieci elektrycznej w celu jej dostosowania do przewidywanych obciążeń związanych z funkcjonowaniem osprzętu LAN / serwerów, montażu podłogi technicznej , szafy IT wraz zasilaniem awaryjnym.

6) Inne cechy dla całości systemu:
- System powinien umożliwiać dostęp wyłącznie autoryzowanym użytkownikom i stacjom roboczym
- System powinien monitować zamawiającemu próbę podłączenia nieautoryzowanej jednostki lub udostępnienie Internetu poza lokal
- Urządzenia składowe muszą charakteryzować się trwałością funkcjonowania i zapewnić konstrukcyjnie min. 6 letni okres eksploatacji
- Sprzęt oraz zastosowana technologia ma spełniać nowoczesne standardy dla tego typu urządzeń, zarówno co do ich specyfikacji technicznych elementów elektronicznych, teleinformatycznych oraz mechanicznych - minimalne wymagania w tym zakresie zostały określone w dalszej części dokumentu
- System powinien zapewnić skalowalność, w przypadku rozszerzenia projektu o kolejnych beneficjentów.
- Zastosowane urządzenia muszą być fabrycznie nowe i pochodzić z oficjalnego kanału sprzedaży
- System w warstwie dostępowej powinien być typu otwartego przez co rozumie się możliwość zastosowania w przyszłości radiowych terminali klienckich pochodzących od różnych producentów.

V. Szczegółowe właściwości i wymagania funkcjonalno-użytkowe

5.1 Przygotowanie dokumentacji projektowej, harmonogramu prac oraz innej niezbędnej dokumentacji

Dokumentacja projektowa winna być kompletna z punktu widzenia celu, któremu ma służyć oraz spełniać wymogi określone przepisami:
- ustawy z dnia 7 lipca 1994r. Prawo Budowlane (Dz. U. z 2010 Nr 243 poz. 1623 ze zm.) oraz wydanych na jej podstawie rozporządzeń,
- ustawy z dnia 16 lipca 2004r. Prawo Telekomunikacyjne (Dz. U. z 2004r. Nr 171, poz. 1800 ze zm.) oraz wydanych na jej podstawie rozporządzeń,
- ustawy z dnia 27 kwietnia 2001r. Prawo Ochrony Środowiska (Dz. U. z 2006r. Nr 129, poz. 902 ze zm.) oraz wydanych na jej podstawie rozporządzeń,
- rozporządzenia Ministra Infrastruktury z dnia 2 września 2004 roku w sprawie szczegółowego zakresu i formy dokumentacji projektowej, specyfikacji technicznych wykonania i odbioru robót budowlanych oraz programu funkcjonalno- użytkowego (Dz. U. z 2004r. Nr 202, poz. 2072 ze zm.),
- powszechnie obowiązującymi przepisami prawa i normami budowlanymi

Roboty budowlane muszą być prowadzone zgodnie z:

- zatwierdzoną przez Zamawiającego dokumentacją projektową,
- przepisami ustawy z dnia 7 lipca 1994r. Prawo Budowlane (Dz. U. z 2010 Nr 243 poz.1623 ze zm),
- przepisami ustawy z dnia 16 lipca 2004r. Prawo Telekomunikacyjne (Dz. U. z 2004r. Nr 171, poz.1800 ze zm.),
- przepisami ustawy z dnia 27 kwietnia 2001r. Prawo Ochrony Środowiska (Dz. U. z 2006r. Nr 129, poz. 902 ze zm.),

Wykonawca zobowiązany jest do opracowania projektu sieci radiowej wraz z niezbędną dokumentacją budowlaną oraz wykonawczą obejmującą teren:

Budzicz , Borów, Brzeźno, Dębnica, Pietrowice Małe, Górowo, Jagoszyce, Krościna Wielka, Ligota Strupińska, Ligotka, Pawłów Trzebnicki, Pększyn, Piotrkowice, Prusice, Raszowice, Skokowa, Strupina, Świerzów, Wszemirów

która powinna zwierać:

- planowanie radiowe

- projekty budowlane i projekty wykonawcze wież i masztów antenowych – kompletne (wraz z branżami)

- projekt wykonawczy budowy sieci szerokopasmowej składający się z następujących elementów:
  - projekt wykonawczy budowy szkieletu sieci
  - projekt wykonawczy budowy warstwy dystrybucji i dostępu
  - projekt instalacji zasilających, logicznych oraz sygnałowych w obiektach w których zostaną zainstalowane punkty dostępowe i/lub dystrybucyjne sieci.
  - projekt wyposażenia oraz konfiguracji głównego węzła sieci z uwzględnieniem odpowiednich urządzeń (serwerów, urządzeń aktywnych) jak również mechanizmów kształtowania usług oraz zarządzania użytkownikami sieci.
  - projekt implementacji mechanizmów bezpieczeństwa sieci
  - monitorowania oraz logowania zdarzeń sieciowych.

Wykonawca zobowiązany jest do zachowania wszelkich, przepisów, norm, regulaminów i wytycznych, które są w jakikolwiek sposób związane z wykonywanymi opracowaniami projektowymi i będzie w pełni odpowiedzialny za przestrzeganie ich postanowień podczas wykonywania opracowań projektowych. Wykonawca jest odpowiedzialny za zorganizowanie procesu wykonywania opracowań projektowych, w taki sposób aby założone cele projektu zostały osiągnięte. Wykonawca będzie przestrzegać praw patentowych i będzie w pełni odpowiedzialny za wypełnienie wszelkich wymagań prawnych odnośnie znaków firmowych, nazw lub innych chronionych praw w odniesieniu do projektów, sprzętu, materiałów lub urządzeń użytych

lub związanych z wykonywaniem opracowań projektowych. Wszelkie straty, koszty postępowania, obciążenia i wydatki wynikłe lub związane z naruszeniem jakichkolwiek praw patentowych przez Wykonawcę pokryje Wykonawca. Dokumentacja projektowa powinna być wewnętrznie spójna i skorygowana we wszystkich branżach i zadaniach wyżej opisanych.

Powinna zawierać optymalne rozwiązania funkcjonalne, techniczne, konstrukcyjne, materiałowe i kosztowe. Wykonawca dokumentacji projektowej powinien uzyskać, własnym staraniem i na własny koszt, wszystkie wymagane przepisami opinie i uzgodnienia.

5.1.1 Wymagania wobec planowania radiowego

W procesie planowania sieci należy wykorzystać oprogramowanie które posiada implementację standardów z zakresu oferowanej łączności radiowej oraz umożliwia precyzyjne uwzględnienie wszystkich aspektów związanych z zaawansowanym systemem radiowym w tym :

- Opcje związane ze stacjami bazowymi i klienckimi (wysokość montażu, moc sygnału, straty w torach antenowych, dobór anten z uwzględnieniem ich charakterystyk oraz pochylenia itd.)
- Symulacje pokrycia użytecznym sygnałem radiowym
- Symulacja połączeń punkt-punkt
- Wykorzystanie szczegółowych map (min. mapy ukształtowania terenu oraz mapy z podziałem na min. 6 klas terenu, tzw. clutter)- należy użyć mapy o rozdzielczości co najmniej 20m dla DTM i clutter
- Możliwość importowania wyników wizji lokalnych, w tym tzw. drive testów, które pozwalają na zoptymalizowanie założonych parametrów modeli propagacyjnego;
- Symulacja przyłączania abonentów – rzeczywistych bądź wygenerowanych losowo, z uwzględnieniem wymaganych przez nich parametrów (wymagane przepływności, niezawodność dostarczenia usług)
- Możliwość eksportowania map zasięgów do formatu akceptowalnego np. przez GoogleEarth, co znacznie ułatwia wizualizację efektów końcowych projektu

5.2 Wieże i maszty telekomunikacyjne oraz inne konstrukcje wsporcze

Poniższe wymagania ilościowe i konstrukcyjne w zakresie robót budowlanych należy traktować jako wymagania minimalne. Zaleca się dokonanie wizji lokalnej na terenach objętych projektem w celu prawidłowego określenia potrzeb w tym zakresie (w tym liczby konstrukcji , wysokości) i prawidłowego skalkulowania kosztów opracowania projektów budowlanych oraz budowy wież i masztów antenowych.

Wymagania podstawowe :

- wszystkie maszty, wieże oraz wsporniki antenowe powinny być wykonane zgodnie z Projektem Wykonawczym, oraz z normami i przepisami obowiązującymi w tym zakresie.
- prace powinny być wykonywane pod nadzorem kierownika budowy z uprawnieniami w zakresie konstrukcyjno-budowlanym
- prace na wysokości powinny być wykonywane przez osoby posiadające aktualne badania lekarskie i przeszkolenie do prac wysokościowych

Wymagania szczegółowe :

Wieża lub maszt dla węzłów dostępowych ……..…… min. 7 kpl

- Wieża lub maszt dostosowany do montażu na gruncie o wysokości do 30 metrów zaprojektowana dla obowiązującej strefy wiatrowej oraz obciążenia użytkowego.
- W uzasadnionych przypadkach dopuszcza się instalacje lekkich masztów na dachach budynków, przy czym wysokość konstrukcji nie może przekroczyć 20 m .
- Wszelkie konstrukcje o wysokości 20 m lub więcej , niezależnie od sposobu posadowienia mogą zostać wykonane jedynie ze stali lub strunobetonu.

Maszty lub wieże dla węzłów dystrybucyjno- dostępowych ……..……min.3 kpl

- Wieża lub maszt z odciągami do instalacji na gruncie o wysokości do 40 m , zaprojektowana dla obowiązującej strefy wiatrowej oraz obciążenia użytkowego.
- Wszelkie konstrukcje o wysokości 20 m lub więcej , niezależnie od sposobu posadowienia mogą zostać wykonane jedynie ze stali lub strunobetonu.

Maszt lub wieża dla każdej lokalizacji powinien być tak dobrany aby wysokość zawieszenia anten zapewniała poprawną obsługę użytkowników końcowych (BO) oraz poprawną transmisję dla połączeń szkieletowych i dystrybucyjnych przy zachowaniu warunku pełnej widoczności optycznej i radiowej .

Zaprojektowane wieże i /lub maszty powinny zapewniać łatwy, tani i bezpieczny dostęp do zainstalowanych na nich urządzeń aktywnych jak również w celu konserwacji samej konstrukcji.

Wsporniki dla radiolinii oraz urządzeń abonenckich ……..…. liczba wg. projektu

- Wspornik o wysokości nie przekraczającej 3m, montowany do ściany szczytowej, trzonu kominowego lub innego miejsca na budynku/budowli zapewniającego prawidłową pracę radiowego urządzenia abonenckiego / radiolinii (parametry opisane w dalszej części opracowania).
- Sposób montażu i miejsce umieszczenia powinny każdorazowo zostać uzgodnione z właścicielem obiektu. Dodatkowo miejsce instalacji wspornika powinno zapewnić optymalne przeprowadzenie okablowania transmisyjnego od radiowego urządzenia abonenckiego do zestawu komputerowego lub szafki sprzętowej.

Wymagania gwarancyjne i serwisowe :

Wykonawca udzieli minimum 36 miesięcznej gwarancji na wykonane konstrukcje.

W okresie gwarancji wykonawca zobowiązuje się do usuwania wszelkich wad i nieprawidłowości powstałych na wskutek normalnej eksploatacji. Jeśli w trakcie okresu gwarancyjnego, istnieje konieczność wykonywania okresowych przeglądów gwarancyjnych, wówczas przeglądy te będą wykonywane na koszt Wykonawcy.

5.2.1 Instalacja szaf teletechnicznych oraz wykonanie instalacji okablowania zasilającego, sygnałowego oraz logicznego pod potrzeby instalacji wyposażenia węzłów sieci (szkieletowych , dystrybucyjnych i dostępowych)

We wszystkich lokalizacjach budowy masztów lub wież telekomunikacyjnych wymagana jest dostawa oraz instalacja szaf teletechnicznych w wykonaniu zewnętrznym lub wewnętrznym (w zależności od potrzeb) z przeznaczeniem na urządzenia aktywne 19''.
Wykonawca powinien zaprojektować szafy o wymiarach i pojemności stosownej do wymagań. Ponadto we wszystkich lokalizacjach, gdzie zostaną zainstalowane elementy infrastruktury, należy wykonać instalacje kablowe (sygnałowe, zasilające logiczne itp.) oraz zainstalować podliczniki w celu rozliczania energii
Lokalizacja szaf oraz sposób prowadzenia instalacji kablowych powinien być wcześniej uzgodniony z właścicielem obiektu.

Prace dodatkowe związane z masztami i wieżami

- w przypadku wież / masztów na gruncie należy wykonać badania geologiczne gruntu

pod budowę konstrukcji (fundamentów)

- Należy wykonać ustalenie z właścicielem nieruchomości warunków przyłączenia i wykonania instalacji elektrycznej . W przypadku montażu liczników / podliczników należy wykonać projekt instalacji elektrycznej.

- w przypadku budowy wieży/masztów na terenie otwartym należy odpowiednio zagospodarować teren wokół obiektu (ogrodzenie , system alarmowy , oświetlenie , tablice z ostrzeżeniem i inne zgodnie z przepisami)

- dla wszystkich masztów i wież Wykonawca dostarczy odpowiednie instrukcje dotyczące ich użytkowania , eksploatacji w szczególności prac konserwacyjnych oraz serwisu urządzeń radiowych .

5.3 Budowa sieci szkieletowej oraz połączeń dystrybucyjnych

5.3.1 Radiolinia min. 200 Mb/s FDX do połączeń szkieletowych …….. .min. 4 kpl.

5.3.2 Radiolinia min. 100 Mb/s FDX do połączeń dystrybucyjnych ……min. 7 kpl.

Wymagania ogólne

- Wykonawca powinien zaproponować taki dobór pasm radiowych, który zapewni najmniejsze opłaty roczne wnoszone do UKE
- Radiolinie powinny obsługiwać pasma licencjonowane: 28,32, 38 ,42 GHz
- System powinien posiadać budowę typu Split, czyli jednostkę Indoorową (IDU) i Outdoorową (ODU), przy czym jednostka Indoorowa powinna być niezależna od częstotliwości.
- System powinien oferować dwukierunkową transmisję z przepływnościami od 4Mbps do ponad 400Mbps dla pojedynczej pary urządzeń tworzących system punkt-punkt poprzez zmianę licencji.
- System powinien oferować możliwość pracy w trybie bez protekcji 1+0 oraz z protekcją mikrofalową typu 1+1 w jednym IDU bez potrzeby wymiany dostarczonego IDU
- System powinien oferować możliwość pracy w trybie XPIC bez potrzeby wymiany dostarczonego IDU
- System powinien pracować w zakresie modulacji min. QPSK- 512QAM
- Ze względu na koszty opłat za pasmo wnoszone do UKE Zamawiający określa następujące przepływności radiolinii w danym kanale:
- dla kanału 14MHz -- nie mniej niż 100Mbp/s
- dla kanału 28 Mhz – nie mniej niż 200 Mbp/s

Indoor Unit (IDU)

- Urządzenie wewnętrzne powinno zapewniać dostęp od frontu do wszelkich interfejsów (ruchowych, zasilających, radiowych, etc), posiadać wentylator chłodzący jednostkę .
- Zarządzanie radiolinią (sieć DCN) powinno wykorzystywać technologię IP.
- System powinien oferować co najmniej dwa porty 10/100/1000Base-T - elektryczne oraz minimum 2 porty SFP 1000Base-X – optyczne (nie dopuszcza się aby porty działały zamiennie)
- System powinien oferować wsparcie dla Class of Service (CoS) zgodnie z IEEE 802.1p.
- System powinien oferować obsługę 8 klas usług (8 kolejek wg. IEEE 802.1D lub 802.1Q).
- Zarządzanie radiolinią w pełnym zakresie powinno odbywać się za pomocą przeglądarki WWW
- System powinien oferować możliwość obsługi QoS na podstawie informacji zawartych w ramce Ethernetowej (PCP), IP (DSCP) lub MPLS (EXP).

Natywny Ethernet

- Natywny Ethernet jest rozumiany jako transport Ethernetu na interfejsie radiowym bez wykorzystania innych technologii jak PDH SDH.
- System powinien oferować transport natywnego Ethernetu w kanałach o szerokości (ETSI) 7-

56MHz z przepływnością powyżej 400Mbps.

Modulacja adaptacyjna

- System powinien oferować bezprzerwową modulację adaptacyjną, która zapewni automatyczną zmianę modulacji odpowiednio do warunków propagacyjnych.
- Modulacja Adaptacyjna powinna być dostępna w kanałach o szerokości (ETSI) 7-56MHz.
- Zmiany schematu modulacji w funkcjonalności Modulacji Adaptacyjnej powinny następować bez przerwy w ruchu zarówno dla części PDH jak i części ruchu Ethernet o wysokim priorytecie.

Outdoor Unit (ODU)

- Jednostka outdoorowa (ODU) powinna zapewniać możliwość montażu zarówno zintegrowanego z anteną jak i odseparowanego.
- Jednostka outdoorowa (ODU) powinna być uniwersalna, tzn. powinna zapewniać wsparcie dla wszelkich pojemności, wszelkich schematów modulacji, modulacji zarówno stałej jak i adaptacyjnej, oraz wszelkich zastosowanych technologii PDH, SDH i Ethernet.

Gwarancja i utrzymanie :

1. Gwarancja na sprzęt radiowy - 3 lata
2. Warunki świadczenia serwisu gwarancyjnego :

- usunięcie awarii krytycznych (przerwa w transmisji) w czasie nie dłuższym niż 24 godziny od chwili przyjęcia zgłoszenia.
- usunięcie pozostałych awarii i usterek lub tymczasowe przywrócenie funkcjonalności sprzętu w czasie nie dłuższym niż 72 godzin od chwili przyjęcia zgłoszenia
- docelowe usunięcie wad i usterek , którym tymczasowo przywrócono funkcjonalność w czasie nie dłuższym niż 1 miesiąc od daty przyjęcia zgłoszenia

5.3.3 Bezprzewodowy most radiowy punkt-punkt …… liczba wg. projektu

Wymagania techniczne

- Urządzenie przeznaczone do zastosowań zewnętrznych typu punkt-punkt (wyposażone w zestaw montażowy),
- Temperatura pracy: od -30C do 75C,
- Wilgotność pracy: 5 to 95%,
- Pamięć: 64MB SDRAM, 8MB Flash,
- Pobór mocy: max. 8 Watt,
- Zasilanie: możliwość zasilania zgodnego z 802.3af,
- Regulacje prawne: CE, RoHS,
- Urządzenie zintegrowane z dwu-polaryzacyjną anteną o zysku minimum 24dBi
    - Częstotliwość pracy: 4.9GHz-6.1GHz
    - Separacja polaryzacji: min. 28dB
    - Max VSRW 1.1:1
    - Szerokość wiązki H: 6 stopni
    - Szerokość wiązki V: 6 stopni
    - Wykonanie z materiału odpornego na promieniowanie UV

- Moduł radiowy o mocy max 27dBm i czułości -96 dBm,
- Urządzenie pracujące w standardzie IEEE 802.11n 2x2 MIMO o zwiększonej wydajności odbiornika i realnej wydajności min. 50 Mbps dla ruchu TCP/IP,
- Pracuje w trybach: router lub bridge,
- Interfejs WiFi wspierający tryby Access Point, Access Point WDS, Client, Client WDS.
- System do centralnego zarządzania min. 10 urządzeniami wraz z niezbędnymi licencjami

Wymagania gwarancyjne i serwisowe

- Urządzenia powinny być objęte minimum 36-miesięczną gwarancją

5.3.4. Przełącznik dystrybucyjny 24 porty 10/100, ……..min. 5 szt.

Wymagania ogólne

- W celu zachowania pełnej kompatybilności i spójności rozwiązania, oraz uproszczenia zarządzania i administracji – zaleca się aby urządzenia aktywne sieci pochodziły od tego samego producenta.
- Zamawiający oczekuje, że sprzęt dostarczony w ramach realizacji umowy będzie sprzętem nowym, nie używanym (dostarczanym) wcześniej w innych projektach.
- Zamawiający oczekuje, że sprzęt dostarczony w ramach realizacji umowy będzie posiadał świadczenia gwarancyjne Wykonawcy oparte na gwarancji wydanej przez producenta lub oficjalnego dystrybutora sprzętu.
- Zamawiający oczekuje, że sprzęt dostarczony w ramach realizacji umowy będzie sprzętem zakupionym w oficjalnym kanale sprzedaży producenta i posiadającym stosowny pakiet usług gwarancyjnych kierowanych do użytkowników z obszaru Rzeczpospolitej Polskiej.

Wymagania techniczne:

Element	**Charakterystyka**
Minimalne wymagania sprzętowe:	• Urządzenie fabrycznie nowe, nieużywane • Obudowa przeznaczona do montażu w szafie 19”. Wysokość obudowy nie większa niż 1 RU. • minimum 4 porty 1GE do połączenia z przełącznikami rdzeniowymi • minimum 24 porty Ethernet 1000BaseT z auto-negocjacją 10/100/1000 • Wymagane jest aby wszystkie powyższe porty mogły działać jednocześnie. • Wydajność przełącznika min. 90 Gb/s i min. 40 Mpps • Urządzenie musi mieć możliwość łączenia przełączników fizycznych w jeden przełącznik wirtualny, traktowany jako jedno urządzenie logiczne z punktu widzenia protokołów routingu, LACP i Spanning Tree. Maksymalna liczba przełączników obsługiwanych w stosie co najmniej 9szt. • Port konsoli - szeregowy RS-232/RJ45 • Port USB
Funkcje warstwy 2	• GARP VLAN Registration Protocol (GVRP) • Rozmiar tablicy MAC minimum 16 000 adresów

.

	• 4000 sieci VLAN • Agregacja portów statyczna i przy pomocy protokołu LACP • Min. 20 grup portów zagregowanych, możliwość stworzenia grupy z min. 8 portów • Spanning Tree: MSTP 802.1s, RSTP 802.1w, STP Root Guard • Obsługa protokołu umożliwiającego budowanie tzw. szybkobieżnych topologii redundantnych, umożliwiającego przełączenie przesyłania danych na ścieżkę zapasową w czasie poniżej 50ms
Bezpieczeństwo	• DHCP snooping • RADIUS • Secure Shell (SSHv2) • IEEE 802.1X– dynamiczne dostarczanie polityk QoS, • Port isolation • Port security: zezwalający na dostęp tylko specyficznym adresom MAC • MAC-based authentication • IP source guard
Quality of Service (QoS)	• Funkcje QoS: kreowanie klas ruchu w oparciu o access control lists (ACLs), IEEE 802.1p precedence, IP, DSCP oraz Type of Service (ToS) precedence; • 8 kolejek QoS per port
Monitoring i diagnostyka	• Port mirroring
Zarządzanie	• Zdalna konfiguracja i zarządzanie przez Web (https) oraz linię komend (CLI) • IEEE 802.1ab LLDP • Serwisy DHCP: Snooping, Security • SNMPv1, v2, v3 • Syslog

Wymagania gwarancyjne i serwisowe

- Urządzenie powinny być objęte minimum 36 miesięczną gwarancją

5.3.5 Zasilacz awaryjny UPS 3000VA (wraz z bateriami) ……..……min. 4 kpl

Wymagania techniczne:

- Moc pozorna 3000VA
- Moc rzeczywista 1800 Wat
- Architektura UPSa line-interactive
- Maksymalny czas przełączenia na baterię 1,5 ms
- Minimalny czas podtrzymywania dla obciążenia 100% - 6 min
- Minimalny czas podtrzymywania dla obciążenia 50% - 15 min
- Urządzenie powinno posiadać układ automatycznej regulacji napięcia AVR
- Urządzenie powinno być wyposażone w port komunikacyjny RS232
- Urządzenie powinno posiadać oprogramowanie do monitorowania parametrów pracy UPSa
- Urządzenie powinno posiadać możliwość rozbudowy poprzez dołożenie dodatkowego modułu bateryjnego
- Urządzenia powinno posiadać obudowę typu Rack 19’’
- Maksymalna wysokość urządzenia wraz z bateria nie może przekroczyć 6U

Wymagania gwarancyjne i serwisowe

- Urządzenie powinny być objęte minimum 36 miesięczną gwarancją.

5.4 Budowa węzłów dostępowych sieci …….min.12 kpl

Planowana jest budowa co najmniej 12 Węzłów Dostępowych, w oparciu o wybudowane wieże/maszty telekomunikacyjne oraz wybrane inne lokalizacje na terenie Gminy Prusice .
Sieć dostępowa powinna być tak zaprojektowana aby objęła swym zasięgiem co najmniej następujące miejscowości: Budzicz , Borów, Brzeźno, Dębnica, Pietrowice Małe, Górowo, Jagoszyce, Krościna Wielka, Ligota Strupińska, Ligotka, Pawłów Trzebnicki, Pększyn, Piotrkowice, Prusice, Raszowice, Skokowa, Strupina, Świerzów, Wszemirów

Wszystkie węzły dostępowe powinny być wyposażone w następujący zestaw elementów i urządzeń:
a) w zakresie infrastruktury pasywnej:
- maszty /wieże telekomunikacyjne dla urządzeń i anten
- szafka dystrybucyjna 19''
- okablowanie zasilające do szaf wraz z podlicznikem energii
- okablowanie logiczne i sygnałowe

b) w zakresie infrastruktury aktywnej
- punkt dostępowy WLAN (802.11a/b/g/n MIMO)
- anteny sektorowe 2,4 GHz i 5GHz wykorzystujące technologię MIMO
- zarządzany przełącznik dostępowy z portami PoE
- zasilacz awaryjny UPS

Poniżej przedstawiono minimalne wymagania techniczne, funkcjonalne i gwarancyjno- serwisowe poszczególnych elementów i urządzeń.

5.4.1 Przełącznik dostępowy 8 port 10/100 8xPoE ……min. 7 szt.

Wymagania techniczne:

Element	Charakterystyka
Minimalne wymagania sprzętowe:	• Urządzenie fabrycznie nowe, nieużywane • Obudowa przeznaczona do montażu w szafie 19". Wysokość obudowy nie większa niż 1 RU. • minimum 1 port 1GE Combo do połączenia z przełącznikami rdzeniowymi • minimum 8 portów Ethernet 1000BaseT z auto-negocjacją 10/100/1000 z obsługą Power over Ethernet w standardzie 802.3af i 802.3at • Wymagane jest aby wszystkie powyższe porty mogły działać jednocześnie. • Wydajność przełącznika min. 8 Gb/s i min. 2,5 Mpps • Przełącznik wyposażony w zasilacz 230V/AC • Port konsoli - szeregowy RS-232
Funkcje warstwy 2	• GARP VLAN Registration Protocol (GVRP) • Rozmiar tablicy MAC minimum 8 000 adresów • 4000 sieci VLAN • Spanning Tree: MSTP 802.1s, RSTP 802.1w, STP 802.1d • Urządzenie musi wpierać obsługę funkcjonalności tzw. Voice VLAN • Urządzenie musi wspierać funkcjonalność podwójnego tagowania VLANów (QinQ)

Konwergencja	• Automatyczna konfiguracja VLANu głosowego • LLDP-MED
Bezpieczeństwo	• DHCP snooping • RADIUS • Secure Shell (SSHv2) • Urządzenie musi wspierać mechanizmy bezpieczeństwa takie jak: 802.1X, SNMPv3, web based authentication, MAC authentication, MFF zgodnie z RFC 4562, BPDU protection, izolacja ruchu w warstwach L2/L3 modelu OSI, wykrywanie pętli na porcie dostępowym, • Guest VLAN • Port isolation • Urządzenie musi mieć możliwość limitowania prędkości przesyłania danych skierowanych do procesora urządzenia.
Quality of Service (QoS)	• Urządzenie musi wspierać priorytezację ruchu zgodnie z 802.1p • Urządzenie musi obsłużyć 4 kolejki dla QoS na każdym porcie • Urządzenie musi umożliwiać zarządzanie zatorami w sieci poprzez przydzielanie każdej kolejce w QoS określonych priorytetów możliwością określenia kolejki priorytetowej (typu strict priority) i kolejek ważonych • Urządzenie musi umożliwiać limitowanie prędkości dla określonych danych (rozróżnianych poprzez adresy IP, porty TCP i UDP, znaczniki 802.1p, IP Precedence
Monitoring i diagnostyka	• Urządzenie musi umożliwiać realizacje funkcji SPAN i RSPAN, czyli kopiowania ruchu z jednego portu na inny port lub do określonego VLANu • Funkcja SPAN musi umożliwiać również kopiowanie ruchu skierowanego do procesora urządzenia oraz kopiowanie ruchu z określonego VLANu • Urządzenie musi posiadać mechanizm do badania jakości połączeń (np. IP SLA) i zbieranie statystyk typu jitter, delay oraz pobieranie tych danych z urządzenia za pomocą protokołu SNMP
Zarządzanie	• Zdalna konfiguracja i zarządzanie przez Web (https) oraz linię komend (CLI) • IEEE 802.1ab LLDP • SNMPv1, v2, oraz v3

Wymagania gwarancyjne i serwisowe

- Urządzenia powinny być objęte minimum 36-miesięczną gwarancją .

5.4.2 Bezprzewodowy punkt dostępu 802.11a/b/g/n ……..……min.18 szt.

Wymagania techniczne

- Urządzenie musi posiadać oprogramowanie do pracy w trybie tzw „lekkiego AP" pod kontrolą kontrolera bezprzewodowego WLAN dostarczonego w ramach niniejszego postępowania i powinny z nim tworzyć spójny i jednorodny system.
- Obsługa WDS
- Obsługa protokołu umożliwiającego oddzielenie ruchu lokalnego (wychodzącego bezpośrednio z AP) od ruchu kierowanego do kontrolera.
- Obsługiwane standardy radiowe:
  - 802.11 a/b/g/n, jednoczesna obsługa minimum 16 ssid
  - moc interfejsów radiowych 20dBm, per antena z możliwością zmniejszenia poziomu
  - obsługa DFS

- obsługa 3x3 MIMO

- Ilość portów:
  - Minimum jeden port RJ-45 auto-sensing 10/100/1000 port (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE802.3ab Type 1000Base-T), umożliwiający pracę w trybie half/full duplex
  - Konsolowy port do zarządzania RJ45
- Urządzenie z możliwością podłączenia anten MIMO w paśmie 2,4Ghz oraz 5Ghz
- Urządzenie musi obsługiwać funkcjonalność „Dying Gasp" umożliwiającą podtrzymanie pracy urządzenia oraz wysłanie alarmu po awarii zasilania do systemu zarządzającego/zbierającego alarmy
- Możliwość uruchomienia równoważonego obciążenia AP opartego o zdefiniowane limity ilości podłączonych urządzeń końcowych lub limitu transferu danych
- Obsługiwana prędkość radiowa do 450Mbps na każdy moduł radiowy
- Pamięć RAM minimum 256MB
- Pamięć flash minimum 32MB
- Temperatura pracy: -10º do +50º C
- Możliwość podłączenia zewnętrznego zasilacza AC 230VAC
- Obsługa zasilania zgodnego z 802.3af
- Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.
- Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich.
- Zamawiający wymaga, aby urządzenia posiadały 3-letni serwis gwarancyjny, świadczony przez Wykonawcę na bazie wsparcia serwisowego producenta.

5.4.3 Anteny do punktów dostępowych ……..……min.36 szt.

Wymagania techniczne

Dobór rodzaju oraz typu anten, powinien być uzależniony od warunków propagacyjnych dla poszczególnych lokalizacji, w których zostaną zainstalowane bezprzewodowe punkty dostępu. Należy jednak stosować anteny sektorowe i/lub dookólne, wykonane w technologii MIMO i przystosowane do zastosowań zewnętrznych. Każdy bezprzewodowy punkt dostępu należy wyposażyć w anteny na pasmo radiowe 2,4 GHz, jak i 5 GHz

- Minimalny wymagany zysk energetyczny dla anten sektorowych to 14 dBi
- Minimalny wymagany zysk energetyczny dla anten dookólnych to 12 dBi

Wymagania gwarancyjne i serwisowe
- anteny powinny być objęte 36-miesięczną gwarancją

5.4.4 UPS 1000VA RACK……..……..min.7 szt.

Wymagania techniczne

- Moc pozorna 1000VA
- Moc rzeczywista 600 W
- Architektura UPSa line-interactive
- Maksymalny czas przełączenia na baterię 1,5 ms
- Minimalny czas podtrzymywania dla obciążenia 100% - 2 min
- Minimalny czas podtrzymywania dla obciążenia 50% - 12 min
- Urządzenie powinno posiadać układ automatycznej regulacji napięcia AVR

- Urządzenie powinno być wyposażone w port komunikacyjny RS232
- Urządzenie powinno posiadać oprogramowanie do monitorowania parametrów pracy UPSa
- Urządzenia powinno posiadać obudowę typu Rack 19''
- Maksymalna wysokość urządzenia 2U

Wymagania gwarancyjne i serwisowe

- urządzenia typu UPS powinny być objęte 36-miesięczną gwarancją.

5.4.5 Bezprzewodowy terminal klienta 802.11 a/n …… liczba wg. projektu

Wymagania techniczne

- Interfejs Ethernet : 100 base-T Ethernet (RJ-45) zgodny z PoE
- LAN Protokół: IEEE 802.3 (CSMA/CD)
- WLAN Protokół Radiowy: IEEE 802.11a/n
- Interfejs WLAN: OFDM, TDD
- Radio:
  - Zakres obsługiwanych częstotliwości: Europa (ETSI): 5500-5700 MHz (11 kanałów) z DFS (automatyczny wybór częstotliwości),
  - Typ modulacji : BPSK, QPSK, 16QAM, 64QAM, HT20, HT40
- Szerokość kanału możliwość ustawienia : 5/10/20/40 MHz
- Zintegrowana antena panelowa dual polar 15 dBi
- Temperatura pracy: -30°C - +70°C

Wymagania gwarancyjne i serwisowe

- terminale powinny być objęte 36-miesięczną gwarancją

5.4.6 Bezprzewodowy terminal klienta 802.11 b/g/n …… liczba wg. projektu

Wymagania techniczne

- Interfejs Ethernet : 100 base-T Ethernet (RJ-45) zgodny z PoE
- LAN Protokół: IEEE 802.3 (CSMA/CD)
- WLAN Protokół Radiowy: IEEE 802.11 b/g/n
- Interfejs WLAN: OFDM, TDD
- Radio:
  - Zakres obsługiwanych częstotliwości: Zakres obsługiwanych częstotliwości: Europa (ETSI): 2400-2483,5 MHz (13 kanałów)
  - Typ modulacji : BPSK, QPSK, 16QAM, 64QAM, HT20, HT40
- Szerokość kanału możliwość ustawienia : 5/10/20/40 MHz
- Zintegrowana antena panelowa dual polar 14 dBi
- Temperatura pracy: -30°C - +70°C

Wymagania gwarancyjne i serwisowe

- terminale powinny być objęte 36-miesięczną gwarancją

5.5 Wyposażenie Głównego Węzła Dystrybucyjnego i Centrum zarządzania siecią szerokopasmową.

5.5.1 Adaptacja pomieszczenia przeznaczonego na Centrum Zarządzania Siecią szerokopasmową

Zakres prac adaptacyjnych będzie obejmował :
a) Roboty budowlane związane z adaptacją pomieszczenia a w szczególności:

- montaż podłogi antyelektrostatycznej poprzez położenie specjalnej wykładziny rozpraszającej ładunki elektrostatyczne, wykładzinę należy zamontować do stabilnego podłoża klejem przewodzącym i połączyć miedzianymi taśmami do miejscowej szyny uziemiającej

- wykonanie miejscowej szyny wyrównawczej oraz jej połączenie przewodem LgYż fi 16 mm z główną szyną uziemienia budynku

- wykonanie ściany działowej wraz z odpowiedniej klasy drzwiami antywłamaniowymi
- modernizacja sieci elektrycznej
- wykonanie przepustów kablowych i sieci LAN

b) Instalację systemu kontroli dostępu ACC w pomieszczeniu serwerowni
c) Dostawę i Instalacje klimatyzatora
d) Dostawę i instalacje szafy teletechnicznej.

Wymagania ogólne dla system dostępu

- System kontroli dostępu powinien być zrealizowany na bazie urządzeń, które będą pozwalać na rejestrację i podgląd zdarzeń wejścia i wyjścia na kontrolowanym przejściu.
- Zdarzenia te powinny być przesyłane do komputera po sieci lokalnej Ethernet.
- System powinien umożliwiać dostęp poprzez wykorzystanie kart zbliżeniowych oraz manipulatora numerycznego.
- System powinien być wyposażony w dodatkowe elementy pozwalające na ochronę pomieszczenia przed niepowołanym dostępem oraz innymi zjawiskami losowymi.
- Na te elementy składają się:
  - Czujnik otwarcia drzwi
  - Czujnik zbicia szkła
  - Sygnalizacja akustyczno optyczna
- System kontroli powinien w sytuacji wykrycia niepowołanego dostępu dokonać alarmowania poprzez uruchomienie sygnalizatora akustyczno optycznego, jak również wysłanie powiadomienia do odpowiednich osób poprzez sieć GSM.
- Należy również dokonać integracji tego systemu z systemem CCTV, w taki sposób, aby detekcja ruchu lub inny zdarzenie wywołujące alarm powodowało włączenie rejestracji zapisu obrazu z kamery usytuowanej w pomieszczeniu lub przed wejściem do niego

Wymagania techniczne:

System kontroli dostępu należy oprzeć na cyfrowej centrali umożliwiającej współpracę zarówno z czujnikami detekcji sygnałów zewnętrznych jak również z urządzeniami kontroli przejść. Centralę należy zainstalować w obudowie natynkowej wyposażonej w transformator oraz akumulator min. 7 Ah. Kontrola przejścia powinna zostać zrealizowana za pomocą zwory elektromagnetycznej zamontowanej w ościeżnicy drzwi. Jeżeli będą zastosowane metalowe drzwi antywłamaniowe, to należy rozważyć montaż rygla elektromagnetycznego zamiast zwory. Zarówno zwora jak i rygiel powinny pracować w trybie rewersowym, oznacza to , że w normalnym trybie pracy urządzenia te powinny być zasilane napięciem, co spowoduje blokadę drzwi. W trybie otwarcia drzwi urządzenia ryglujące powinny być w stanie jałowym. Przy drzwiach wejściowych należy umieścić czytnik linii papilarnych lub kart zbliżeniowych oraz manipulator. Manipulator należy montować w kasecie natynkowej zamykanej na kluczyk. Manipulator oraz kaseta powinny zostać wyposażone w styk antysabotażowy. Po przyłożeniu karty zbliżeniowej lub zeskanowaniu linii papilarnych do czytnika powinno nastąpić zwolnienie zwory i uzyskanie dostępu do pomieszczenia. Takie zdarzenie dostępu powinno zostać zarejestrowane w buforze centrali i przesłane do systemu monitorującego przejścia. System powinien umożliwiać przegląd zdarzeń i weryfikacje użytkowników wchodzących do pomieszczenia, z możliwością odczytania tych zdarzeń na co najmniej 1 miesiąc wstecz. Wyjście z pomieszczenia powinno następować po wciśnięciu przycisku wewnątrz pomieszczenia. Nie jest wymagana rejestracja wyjścia z pomieszczenia. System powinien być wyposażony w dodatkowe czujniki monitorujące stan otoczenia. Centrala w stanie zazbrojenia powinna reagować na zdarzenia niepowołanego dostępu poprzez zastosowanie czujników ruchu, otwarcia drzwi, zbicia szyby.

Każde zarejestrowane zdarzenie naruszenia strefy chronionej powinno generować alarm akustyczno optyczny, jak również wysyłać komunikat do centrum powiadamiania lub do przydzielonych numerów telefonicznych z wykorzystaniem linii analogowej. System powinien umożliwiać przyłączenie do niego zewnętrznej linii telefonicznej analogowej. System powinien zostać wyposażony również w czujnik dymu, co powinno dawać dodatkową możliwość alarmowanie o zagrożeniu pożarowym do centrali alarmowej lub do centrali p.poż. Proponowany system kontroli dostępu powinien charakteryzować się modularnością, możliwością jego rozbudowy i modyfikacji. Powinien dawać możliwość rozbudowy systemu o dodatkowe przejścia jak również dodatkowe elementy ochrony, nie powinien to być system zamknięty. Powinien dawać możliwości konfiguracyjne pozwalające na dostosowanie parametrów pracy do indywidualnych wymagań.

Wymagania formalne gwarancyjne i serwisowe

- na wszystkie prace budowlane oraz na instalację systemu kontroli dostępu wymagana jest minimum 36 miesięczna gwarancja.

5.5.2 Przełącznik szkieletowy L3 …….. 1 szt.

Wymagania techniczne

Element	Charakterystyka
Minimalne wymagania sprzętowe:	• Urządzenie fabrycznie nowe, nieużywane • Obudowa przeznaczona do montażu w szafie 19”. Wysokość obudowy nie większa niż 1 RU. • minimum 4 porty 1GE SFP do połączenia z przełącznikami rdzeniowymi • minimum 24 porty Ethernet 1000BaseT z auto-negocjacją 10/100/1000 z obsługą Power over Ethernet w standardzie 802.3af i 802.3at • Wymagane jest aby wszystkie powyższe porty mogły działać jednocześnie. • Wydajność przełącznika min. 140 Gb/s i min. 90 Mpps • Przełącznik wyposażony w 2 wbudowane zasilacze 230V/AC, każdy o mocy minimum 450W. • Możliwość wymiany zasilaczy w trakcie pracy urządzenia bez wpływu na jego działanie • Urządzenie musi mieć możliwość łączenia przełączników fizycznych w jeden przełącznik wirtualny, traktowany jako jedno urządzenie logiczne z punktu widzenia protokołów routingu, LACP i Spanning Tree. Maksymalna liczba przełączników obsługiwanych w stosie co njamniej

	9szt. • Przełączanie w warstwie drugiej i trzeciej modeli ISO/OSI. • Port konsoli - szeregowy RS-232
Funkcje warstwy 2	• GARP VLAN Registration Protocol (GVRP) • Rozmiar tablicy MAC minimum 16 000 adresów • 4000 sieci VLAN • Agregacja portów statyczna i przy pomocy protokołu LACP • Min. 20 grup portów zagregowanych, możliwość stworzenia grupy z min. 8 portów • Spanning Tree: MSTP 802.1s, RSTP 802.1w, STP Root Guard
Funkcje warstwy 3	• routing IPv4 z prędkością łącza, • wsparcie dla routingu IPv4: statycznego , RIP i RIPv2, OSPF, IS-IS i BGP • routing IPv6 z prędkością łącza, • wsparcie dla routingu IPv6: statycznego RIPng, OSPFv3 • Rozmiar tablicy routingu 12 000 wpisów • Virtual Router Redundancy Protocol (VRRP) • Policy-based routing • IGMPv1, v2, and v3 • PIM-SSM, PIM-DM i PIM-SM (dla IPv4 i IPv6) • Equal-Cost Multipath (ECMP)
Konwergencja	• Automatyczna konfiguracja VLANu głosowego • LLDP-MED
Bezpieczeństwo	• DHCP snooping • RADIUS • Secure Shell (SSHv2) • IEEE 802.1X– dynamiczne dostarczanie polityk QoS, ACLs i sieci VLANs: zezwalające na nadzór nad dostępem użytkownika do sieci • Guest VLAN • Port isolation • Port security: zezwalający na dostęp tylko specyficznym adresom MAC • MAC-based authentication • IP source guard • URPF • Obsługa min. 63 instancji VRF
Quality of Service (QoS)	• Funkcje QoS: kreowanie klas ruchu w oparciu o access control lists (ACLs), IEEE 802.1p precedence, IP, DSCP oraz Type of Service (ToS) precedence; • 8 kolejek QoS per port
Monitoring i diagnostyka	• Port mirroring
Zarządzanie	• Zdalna konfiguracja i zarządzanie przez Web (https) oraz linię komend (CLI) • IEEE 802.1ab LLDP • Pamięć flash o pojemności pozwalającej na przechowywanie minium dwóch wersji oprogramowania systemowego • Serwisy DHCP: serwer, klient i relay • SNMPv1, v2, and v3 • Syslog

Wymagania gwarancyjne i serwisowe

- Urządzenie powinny być objęte minimum 36 miesięczną gwarancją.

5.5.3 Urządzenie bezpieczeństwa sieciowego ……1 szt.

Wymagania techniczne

Element	Charakterystyka
Minimalne wymagania sprzętowe:	• Urządzenie fabrycznie nowe, nieużywane. • Obudowa musi być wykonana z metalu. Ze względu na różne warunki, w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowanie wykonanej z tworzywa. • Obudowa przystosowana do montażu w szafie rack 19". • Wymagane są minimum 2 porty typu WAN/LAN Combo 10/100/1000Base-T RJ45 (100/1000 Base-X SFP) • Wymagane jest aby wszystkie powyższe porty mogły działać jednocześnie. • Urządzenie wyposażone w zasilacz 230V/AC. • Wymagana jest wydajność urządzenia minimum 800 Mbps. • Wymagana jest Ilość jednocześnie obsługiwanych połączeń minimum 600.000 • Wymagana jest wydajność połączeń IPSec VPN minimum 300 Mbps. • Wymagana jest ilość jednocześnie obsługiwanych tuneli IPSec VPN minimum 2.000. • Wymagana jest wydajność modułu IPS minimum 350 Mbps. • Wymagana jest ilość jednocześnie obsługiwanych tuneli SSL VPN minimum 3. • Wymagana jest obsługa trzech trybów pracy: routing mode, transparent mode, composite mode • Wymagana jest obsługa minimum 10 wirtualnych Firewalli.
Funkcje warstwy 3	• Obsługa routingu IPv4 i IPv6. • Obsługa routingu statycznego.
Firewall	• Obsługa pełnej funkcjonalności NAT a w szczególności: source IP address NAT, destination IP address NAT, static IP address NAT, IP pool NAT. • Wsparcie dla następujących protokółów: FTP ALG,SIP ALG,ICMP ALG ,NetBios ALG. • Ochrona przed atakami: SYN flood, ICMP flood, UDP flood, IP Spoofing, LAND attack, Smurf attack, Fraggle attack, Winnuke attack, Ping of Death attack, Tear Drop attack, address scanning attack, port scanning attack, IP Option control attack, IP packet fragmentation control attack, TCP label validity check attack, ICMP redirection packet attack, ICMP unreachable packet attack i TRACERT packet • Możliwość kontroli ruchu P2P: protocol-based P2P , policies-based p2p dla konkretnego klienta. • Wsparcie dla: static black list i dynamic black list. • Wsparcie dla: routingu statycznego. • Wsparcie: SSL VPN,IPSEC VPN. • Jeżeli funkcja SSL VPN wymaga dodatkowej licencji wymaga się dostarczenia odpowiedniej licencji na okres 3 lat.
Zarządzanie	• Zdalna konfiguracja i zarządzanie przez Web (https) oraz SSL • Dostęp administracyjny do urządzenia poprzez CLI i SSH

Wymagania gwarancyjne i serwisowe

- Urządzenie powinny być objęte minimum 36 miesięczną gwarancją.

5.5.4 Kontroler sieci bezprzewodowej WLAN ……1szt.

Wymagania techniczne:

- Standardy radiowe: 802.11a, 802.11b, 802.11g, 802.11n z późniejszym wsparciem dla 802.11ac
- Sprzętowe:
  - Kontroler powinien posiadać metalową samodzielną obudowę, max 1RU

    - Minimum 2 porty SFP+
    - Minimum 24 porty Gigabit Ethernet 10/100/1000 RJ45 (Auto-MDIX) z obsługą standardów 802.3af i 802.3at
- Urządzenie musi posiadać możliwość zainstalowania zasilaczy typu: AC, DC oraz zasilaczy AC posiadający minimum 360W mocy dla funkcjonalności PoE
- Urządzenie musi posiadać możliwość zainstalowania wewnętrznego zasilacza redundantnego. Nie dopuszcza się rozwiązania zewnętrznego
- Dostarczone urządzenie musi zostać wyposażone w jeden zasilacz AC
- Podłączanie AP
    - Podłączanie z użyciem L2 (L2 radio adoption)
    - Podłączanie AP poprzez sieć routowanę IP (L3 radio adoption), wykrywanie poprzez konfigurację DNS oraz opcje w DHCP
- Wydajność
    - Obsługa minimum 18 AP, możliwość rozbudowy do 512AP poprzez dołożenie licencji
    - Minimum 1000 ESSID
    - Minimum 4000 sieci VLAN
- Uwierzytelnianie
    - IEEE 802.1x RADIUS server authentication, wbudowany Web portal
    - WPA/WPA2 with PSK, EAP-MD5, EAP-TLS, PEAP
- Szyfrowanie
    - 64/128 WEP keys, WPA/WPA2 with CCMP/TKIP
    - Dynamic session key management
- Kontrola dostępu i jakość ruchu
    - MAC address filtering, access control lists, DSCP
    - QoS wielopoziomowa kontrola pasma
    - Mapowanie SSID na VLAN (do min 16 jednoczesnych SSID)
- Zarządzanie: WWW (HTTPS), SNMP v.2, v3, CLI
- Tryby pracy
    - Praca AC w trybie wysokiej dostępności (HA), opartej na protokole VRRP ze wsparciem BFD (lub równoważne) co umożliwia szybkie przełączenie na kontroler zapasowy bez zerwania połączenia access-pointów z kontrolerem
    - Możliwe uruchomienie trybu HA z opcją równoważonego obciążenia kontrolerów
    - Praca AP w trybie lokalnym (dane użytkowników przesyłane lokalnie)
    - Praca AP w trybie centralnym (dane użytkowników przesyłane przez tunel CAPWAP do kontrolera)
- Wsparcie dla mechanizmów bezpieczeństwa takich jak DHCP snooping w trybie lokalnym
- Pozostałe
    - DHCP serwer
    - Lokalna baza użytkowników, współpraca z zewnętrznymi serwerami RADIUS
    - DHCP relay
    - LLDP
    - pełny roaming w ramach kontrolera, (L2 i L3)
- Bezpieczeństwo
    - Szyfrowanie DTLS dla kanału kontrolnego w tunelu CAPWAP
    - Identyfikacja urządzeń końcowych (podanie informacji o producencie urządzenia i uruchomionym systemie operacyjnym). Funkcjonalność powinna działać bez uruchamiania dodatkowych serwerów
    - Wykrywanie i obrona przed obcymi access-pointami
    - Wsparcie dla systemu WIPS/WIDS, ochrona przed łamaniem klucza PSK, atakami typu „flood", „spoofing", „weak IV"
- Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.

- Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich.
- Zamawiający wymaga, aby system sterowania siecią bezprzewodową posiadał 3-letni serwis gwarancyjny, świadczony przez Wykonawcę na bazie wsparcia serwisowego producenta lub dystrybutora.

5.5.5 Szafa 42U z wyposażeniem ……..1 szt.

Wyposażenie
Szafa serwerowa 42U szer:800mm głeb:1000mm
Drzwi przednie przeszklone
Drzwi tylne perforowane z blachy, boki z blachy pełnej
Cokół 100 mm z możliwością poziomowania
Panel wentylacyjny dachowy z termostatem i 4 wentylatorami
Zaślepka filtracyjna w otworach podstawy szafy
Półka 2U 400 mm na urządzenia desktop
Półka ruchoma pod klawiaturę
Listwa zasilająca 19" z filtrem 2 szt

5.5.6 Zasilacz awaryjny UPS 3000VA z zestawem baterii …….……..…….min.2 kpl

Wymagania techniczne:
- Moc pozorna 3000VA
- Moc rzeczywista 1800 W
- Architektura UPSa line-interactive
- Maksymalny czas przełączenia na baterię 1,5 ms
- Minimalny czas podtrzymywania dla obciążenia 100% - 6 min
- Minimalny czas podtrzymywania dla obciążenia 50% - 15 min
- Urządzenie powinno posiadać układ automatycznej regulacji napięcia AVR
- Urządzenie powinno być wyposażone w port komunikacyjny RS232
- Urządzenie powinno posiadać oprogramowanie do monitorowania parametrów pracy UPSa
- Możliwość zainstalowania dodatkowego modułu baterii
- Urządzenia powinno posiadać obudowę typu Rack 19''

Wymagania gwarancyjne i serwisowe
- Urządzenie powinny być objęte minimum 36 miesięczną gwarancją..

5.5.7 Serwery i urządzenia dodatkowe

Wymagania techniczne (sprzętowe oraz systemowe):

5.5.7.1 Platforma do wirtualizacji środowisk serwerowych ……..(1 szt.)

LP	Nazwa komponentu	Minimalne wymagania

1	Obudowa	-Typu Rack, wysokość obudowy 4U (obudowa musi umożliwiać konwersję do obudowy wolnostojącej typu tower); -Dostarczony z szynami montażowymi do szafy rack umożliwiającymi pełne wysunięcie serwera oraz z ramieniem podtrzymującym kable;
2	Płyta główna	-Dwuprocesorowa -Minimum 5 złącz PCI Express Gen.3 w tym minimum 2 złącza o prędkości x16 Gen.3 oraz minimum 1 złącze PCI 32bit; -Możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora (niezależne od dysków twardych);
3	Procesory / Wydajność	-Zainstalowane dwa procesory w architekturze x86 osiągające w oferowanym serwerze w testach wydajności SPECint_rate2006 min. 365 pkt; -Wymagane dołączenie do oferty pełnego protokołu testów SPEC dla oferowanego modelu serwera wyposażonego w oferowane procesory (protokół poświadczony przez Wykonawcę)
4	Pamięć RAM	-Zainstalowane 32 GB pamięci RAM -Wsparcie dla technologii zabezpieczania pamięci Advanced ECC, Memory Scrubbing, SDDC; -Wsparcie dla konfiguracji pamięci w trybie „Rank Sparing”; -12 gniazd pamięci RAM na płycie głównej, obsługa minimum 192GB pamięci RAM;
5	Kontrolery dyskowe, I/O	-Zainstalowany kontroler SAS 2.0 RAID 0,1,5,6,50,60, 512MB pamięci podręcznej cache,
6	Dyski twarde	-Zainstalowane 3 dyski SAS 2.0 o pojemności 600 GB każdy,15K RPM, dyski Hotplug; -Minimum 4 wnęki dla dysków twardych Hotplug w dostarczonej konfiguracji;
7	Inne napędy zintegrowane	-Zintegrowany napęd DVD-RW
8	Kontrolery LAN	-2x 1Gb/s LAN, ze wsparciem iSCSI i iSCSI boot, RJ-45;
9	Porty	-zintegrowana karta graficzna ze złączem VGA; -9x USB 2.0, w tym minimum 2 na panelu przednim i minimum 4 na panelu tylnym; minimum jedno USB 2.0 wewnętrzne umożliwiające instalację pendrive; -1x RS-232;
10	Zasilanie, chłodzenie	-Redundantne zasilacze hotplug o sprawności 94% o mocy maksymalnej 450W; -Redundantne wentylatory;
11	Zarządzanie	-Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera – minimum sygnalizacja (poprawna praca/usterka) dla komponentów jak: procesor, wentylatory, dyski twarde, temperatura wewnątrz obudowy, pamięci, zasilaczy; sygnalizacja pracy (zasilania), sygnalizacja identyfikacji (włączana zdalnie) -Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; • Dedykowana karta LAN 1 Gb/s RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; • Dodatkowe złącze serwisowe RJ-45 1Gb/s dostępne z przodu obudowy • Dostęp poprzez przeglądarkę Web (także SSL, SSH) • Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii • Zarządzanie alarmami (zdarzenia poprzez SNMP) • Możliwość przejęcia konsoli tekstowej • Możliwość przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie

		sprzętowym (cyfrowy KVM) • Oprogramowanie zarządzające i diagnostyczne umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.).
12	Wspierane systemy operacyjne	-Windows 2008 R2 Hyper-V, Windows 2012 Hyper-V VMWare, Suse SLES11, RHEL 6
13	Gwarancja	- 3 lata gwarancji , serwis w miejscu instalacji sprzętu, - Czas reakcji na zgłoszenie serwisowe- w następny dzień roboczy po otrzymaniu zgłoszenia. -Dostępność części zamiennych przez 5 lat od momentu zakupu serwera;
14	Dokumentacja, inne	- Elementy, z których zbudowane są serwery muszą być certyfikowane przez jego producenta oraz muszą być objęte gwarancją, potwierdzoną przez oryginalne karty gwarancyjne; - Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego - Oferent zobowiązany jest dostarczyć wraz z ofertą kartę produktową oferowanego serwera umożliwiającą weryfikację parametrów oferowanego sprzętu; - Ogólnopolska, telefoniczna infolinia/linia techniczna, (ogólnopolski numer o zredukowanej odpłatności 0-800/0-801, w ofercie należy podać nr telefonu) w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; -Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;
15	Zainstalowany system operacyjny	System operacyjny zainstalowany na dostarczonym serwerze posiadający następujące funkcjonalności: • Licencja na oprogramowanie musi być przypisana do każdego procesora fizycznego serwera. • Liczba rdzeni procesorów i ilość pamięci nie mogą mieć wpływu na liczbę wymaganych licencji. • Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. • Możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym • Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny. • Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania min. 8000 maszyn wirtualnych. • 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. • Wsparcie dodawania i wymiany pamięci RAM bez przerywania pracy. • Wsparcie dodawania i wymiany procesorów bez przerywania pracy.

		• Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. • Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading lub równoważne. • Wbudowane wsparcie instalacji i pracy na wolumenach, które: a. pozwalają na zmianę rozmiaru w czasie pracy systemu, b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) wgląd w poprzednie wersje plików i folderów, c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d. umożliwiają zdefiniowanie list kontroli dostępu. e. Wbudowany mechanizm klasyfikowania i indeksowania plików w oparciu o ich zawartość. f. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny tj. wydany przez agendę rządową zajmującą się bezpieczeństwem informacji. g. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów h. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. i. Graficzny interfejs użytkownika. j. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, k. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji l. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). m. Możliwość zdalnej konfiguracj i, administrowania oraz aktualizowania systemu. n. Dostępność bezpłatnych narzędzi umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. o. Serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management). p. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b. 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. c. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej

		d. 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. e. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). f. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. g. Serwis udostępniania stron WWW. h. Wsparcie dla protokołu IP w wersji 6 (IPv6), i. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach, j. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. k. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności l. Mechanizmy wirtualizacji mają zapewnić 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 - Wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku różnych dostawców poprzez otwarty interfejs API. - Kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model) m. 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. n. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). o. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. p. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. q. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management. r. Materiały edukacyjne w języku polskim.

Wymagania ogólne dotyczące instalacji oprogramowania na serwerze:

Na dostarczonym serwerze należy zainstalować oraz skonfigurować następujące oprogramowanie:

- instalacja oraz konfiguracja środowiska wirtualizacji serwerów
- instalacja oraz konfiguracja systemu do scentralizowanego zarządzania infrastrukturą maszyn wirtualnych

- utworzenie oraz konfiguracja maszyny wirtualnej dla systemu monitoringu stanu sieci
- dostawa, instalacja oraz konfiguracja systemu będącego środowiskiem dla oprogramowania spełniającego funkcje systemu Monitoringu na maszynie wirtualnej
- utworzenie oraz konfiguracja maszyny wirtualnej dla systemu LMS (ang. *Lan Mangement System*; System Zarządzania Siecią)
- dostawa, instalacja oraz konfiguracja systemu będącego środowiskiem dla oprogramowania LMS na maszynie wirtualnej
- utworzenie oraz konfiguracja maszyny wirtualnej dla systemu zarządzania pasmem
- dostawa, instalacja oraz konfiguracja systemu będącego środowiskiem dla oprogramowania „TrafficManager"

a) System monitoringu infrastruktury sieciowej (1 kpl.)

Wymagania funkcjonalne systemu monitoringu stanu sieci:

Należy dostarczyć narzędzia do sprawnej analizy stanu sieci, w szczególności posiadające następującą funkcjonalność:

- system do diagnostyki oraz wizualizacji bieżącej pacy systemu
- wizualizacja awarii sieci w czasie rzeczywistym
- alarmowanie o awariach (dźwiękowe/ email/ graficznie)
- przeglądanie historii niedostępności usług urządzeń
- monitorowanie przeciążenia sieci
- możliwość monitorowania wszelkich urządzeń sieciowych
- możliwość monitorowania różnych usług udostępnianych przez urządzenia sieci oraz ich dostępność (wykorzystanie zestawu funkcji protokołów ICMP, SNMP protokołów aplikacyjnych)
- monitorowanie SNMP umożliwiające zbieranie szeregu parametrów pracy i statystyk urządzeń sieciowych
- możliwość uzyskania aktualnej informacji o urządzeniu przez wskazanie lub kliknięcie na nie myszką
- dostępność w całej sieci z uprawnionych stacji z zainstalowanymi agentami
- funkcje archiwizacji ustawień oraz danych oprogramowania
- zbieranie logów po protokole SYSLOG
- analiza zdarzeń SYSLOG z opisem znaczenia danego zdarzenia i sugestią rozwiązania danego problemu

b) System zarządzania usługami i użytkownikami sieci „LMS" (1 kpl.)

Wymagania funkcjonalne systemu LMS:

Wymagana jest dostawa oraz konfiguracja specjalizowanego oprogramowania (wraz z wszelkimi niezbędnymi licencjami) tworzącego system zarządzania oraz administracji usługami dostępu do Internetu oraz użytkownikami sieci.

System ten powinien cechować się następującą funkcjonalnością:

- wszelkie dane systemu takie jak: definicje usług, użytkowników, administratorów, urządzenia oraz adresacji sieci przechowywane w bazie SQL
- udostępniona dokumentacja wraz z strukturą drzewa bazy
- dane bazy udostępnione i wykorzystywane przez wszystkie elementy składowe systemu LMS

- przyjazny intuicyjny graficzny interfejs zrealizowany w technologii WWW - udostępniony w sieci zarządzania poprzez protokół http/https
- zarządzanie dostępem do usług (w tym kontrola pasma i statystyk, możliwość prostego włączenia/wyłączenia dostępu do usługi) – tworzenie taryf z definicja parametrów upload/download, ilość połączeń na sekundę, limit danych
- współpraca z zaproponowanym systemem „TrafficManager" – generowanie kolejkowania ruchu w oparciu o zdefiniowane w bazie usługi oraz „klientów" sieci
- ewidencja sprzętu sieciowego – urządzeń sieci (nazwa, model, producent, numer seryjny, hasla dostepu, data zakupu, okres gwarancji, ilosc portow, lokalizacja, itp.) oraz urządzeń dostępowych klienta
- ewidencja adresacji sieci – ip, mac
- inwentaryzacja połączeń urządzeń sieciowych, tworzenie powiązań z urządzeniami klienckimi podłączonymi do urządzeń dostępowych oraz możliwość graficznej prezentacji tak zdefiniowanych połączeń
- przechowywanie danych klientów, konfiguracja usługi, przechowywanie informacji o urządzeniach dostepowch klienta, generowanie oraz przetrzymywanie dokumentów klienta (np. umowa, protokóły)
- korespondencja seryjna
- zarządzanie kontami oraz hostingiem np. kona pocztowe,
- zarządzanie informacja o dodatkowych usługach: mail, ftp, voip itp.
- system obsługi zgłoszeń oraz wyjazdów serwisowych
- archiwizacja danych
- platforma kontaktu z abonentem
- zarządzanie administratorami oraz prawami dostępu do poszczególnych funkcjonalności systemu
- możliwość prostego wyszukiwania urządzeń, adresów IP czy klientów
- serwer typu RADIUS pozwalający na autentykację w oparciu o dane z bazy danych SQL

c) System zarządzania pasmem „TrafficManager" (1 kpl.)

Wymagania funkcjonalne systemu „TrafficManager":

Należy dostarczyć oraz skonfigurować oprogramowanie pełniące role bramy dla klienckich sieci dostępowych oraz nakładającego na ruch wychodzący oraz wchodzący z Internetu odpowiednie polityki kształtowania ruchu zgodnie ze zdefiniowanymi w systemie LMS usługami oraz stacjami końcowymi.

Oprogramowanie musi posiadać następujące cechy i funkcje:

- Kontrola dostępu – nakładanie polityki uprawnień dostępu
  - ✓ sprawdzenie poprawności adresu MAC, IP
  - ✓ zabronienie dostępu odłączonym klientom
  - ✓ możliwość autentykacji użytkownika na podstawie logowania WWW lub PPPoE z użyciem par użytkownik/hasło z bazy danych LMS
  - ✓ wyświetlanie komunikatów w przeglądarce WWW
- Zapewnienie parametrów jakościowych zdefiniowanej w systemi LMS usługi – wdrażanie polityk kształtowania i zarządzania pasmem
  - ✓ dyscypliny kolejkowania – możliwość wyboru typu mechanizmu kolejkowania w kolejkach głównych, usługowych, oraz klienckich
  - ✓ klasy – możliwość grupowania i priorytetyzowania określonego typu ruchu
  - ✓ filtry – filtrowanie ruchu z wykorzystaniem szybkich filtrów haszujących zapewniających wydajność nawet w przypadku bardzo dużej liczby reguł

- ✓ możliwość klasyfikowania ruchu za pomocą filtrów warstwy aplikacji (np. ruch P2P)
- ✓ generowanie klas ruchu dla aktywnych klientów z bazy LMS
- ✓ limitowanie ilości połączeń użytkownika sieci – zgodnie z definicja taryfy w systemie LMS
- ✓ możliwość ustalenia różnych limitów na dzień/noc
- ✓ limitowanie wielkości transferu dla dowolnego okresu czasu

- Zbieranie informacji o przesyłanych danych
  - ✓ tworzenie logów ruchu przechodzącego przez system
  - ✓ logowanie informacji oraz blokowanie klientów przesyłających SPAM
- Tworzenie graficznych statystyk transferów (sieci oraz indywidualnych użytkownika) oraz obciążenia zasobów systemu
- Zabezpieczenia dostępu do sieci
  - ✓ kontrola dostępu terminali klienckich
  - ✓ odseparowanie ruchu sieci zaradzania od sieci klienckich oraz sieci Internet
  - ✓ konfiguracja blokad ruchu z sieci klienckich oraz Internet do panelów zarządzania systemem TrafficManager
  - ✓ konfiguracja blokad ruchu miedzy sieciami klienckimi
  - ✓ ochrona przed atakami DoS
  - ✓ zabezpieczenia przed skanowaniem portów i nieautoryzowanym dostępem
- automatyczny backup konfiguracji, możliwość łatwego eksportu/importu konfiguracji z poziomu graficznego panelu administracyjnego

5.5.7.2 Dostawa i instalacja systemu pamięci masowej …….(1 szt.)

Nazwa komponentu	Wymagane minimalne parametry techniczne
System operacyjny	dedykowany, typu embedded
Procesor	klasy x86, dedykowany do pracy w komputerach stacjonarnych uzyskujący przy pracy w nominalnych warunkach w teście Passmark CPU Mark wynik min. 1000 punktów (wynik zaproponowanego procesora musi znajdować się na stronie http://www.cpubenchmark.net, z której wydruk należy dołączyć do oferty)
Pamięć	nieulotna 128 MB typu Flash, operacyjna 1 GB
System dyskowy	- dostępne 4 kieszenie hot-swap z możliwością fizycznej blokady - zainstalowane 4 dyski hot-swap dedykowane do pracy w serwerach, każdy po 2TB - bezpieczeństwo na poziomie RAID 0/ 1/ 5/ 6/ 5+ hot spare, JBOD - system plików ext3, ext4 (dyski wewnętrzne), ext3, ext4, NTFS, FAT32, HFS+ (dyski zewnętrzne)
Interfejsy	- 2 x Gigabit Ethernet z obsługą iSCSI - 3 x USB 2.0
Obudowa	- wysokość maksymalnie 1U dedykowana do montażu w szafie rack 19" z zestawem szyn mocujących - dwa zasilacze redundantne - przyciski: Power, USB One-Touch-Backup, reset
Wspierane systemy operacyjne	Windows 2000, XP, Vista (32-/ 64-bit), Windows 7 (32-/ 64-bit), Windows Server 2003/ 2008, Apple Mac OS X, Linux, Unix
Obsługiwane protokoły	TCP/IP, DHCP client, DHCP server, CIFS/SMB, AFP, NFS, HTTP, HTTPS, FTP, DDNS, NTP, wsparcie Gigabitowych ramek Jumbo, ustawienia Multi-IP, równoważenie obciążenia, Network Service Discovery (UPnP & Bonjour)

Zarządzanie	ograniczenie dostępnej pojemności dysku dla użytkownika, Windows AD, zarządzanie kontami użytkowników (maksymalnie 4096 użytkowników), zarządzanie grupą użytkowników (maksymalnie 512 grup), tworzenie zestawów użytkowników
Dodatkowe oprogramowanie	oprogramowanie do tworzenia obrazów dysku, przywracania systemu od podstaw, szybkiego odzyskiwania bez konieczności ponownego instalowania systemu operacyjnego i aplikacji, zawierające: - rozbudowane funkcje katalogowania do łatwego przeglądania, wyszukiwania i przywracania różnych wersji poszczególnych plików z kopii zapasowych obrazów - szybkie, jednoczesne, bezagentowe operacje tworzenia kopii zapasowych i odzyskiwania maszyn wirtualnych - możliwość tworzenia kopii zapasowych i odzyskiwania danych na nieograniczonej liczbie maszyn wirtualnych działających na hoście, a także wykonywanie migracji typu V2P i P2V . Ilość licencji: 2
Gwarancja	3 lata gwarancji świadczonej w miejscu eksploatacji sprzętu - czas reakcji serwisu: do końca następnego dnia roboczego

5.5.7.3 Stacja do zarządzania ……..(1 szt.)

Komputer stacjonarny przeznaczony zadań administracyjnych, dedykowany obsługi baz danych, programowania współbieżnego, dostępu do sieci Internet, aplikacji biurowych i grafiki prezentacyjnej	
Nazwa atrybutu	Wymagane minimalne
Wydajność	Procesor klasy x86, dedykowany do pracy w komputerach stacjonarnych uzyskujący przy pracy w nominalnych warunkach w teście Passmark CPU Mark wynik min. 4100 punktów (wynik zaproponowanego procesora musi znajdować się na stronie http://www.cpubenchmark.net, z której wydruk należy dołączyć do oferty), zaś komputer w oferowanej przez Wykonawcę konfiguracji testowany przy rozdzielczości monitora min. 1600 x 900 powinien osiągać w teście wydajności SYSMark2012 Office Productivity wynik min. 130 pkt oraz SYSMark2012 System Management wynik min. 124 pkt (szczegółowy raport z przeprowadzonych testów należy dołączyć do oferty). Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testów Wykonawca musi dostarczyć zamawiającemu oprogramowanie testujące oraz oferowany przez siebie zestaw komputerowy z monitorem w terminie nie dłuższym niż 7 dni od otrzymania zawiadomienia od Zamawiającego
Pamięć	min. 4GB pamięci operacyjnej (możliwość rozbudowy do 32GB pamięci) min. 500GB pamięci masowej SATA
Grafika	Komputer w oferowanej przez Wykonawcę konfiguracji testowany przy rozdzielczości monitora min. 1600 x 900 powinien osiągać w teście wydajności SYSMark2012 3D modeling wynik co najmniej 130 pkt. (szczegółowy raport z przeprowadzonych testów należy dołączyć do oferty).
Napędy wbudowane	Nagrywarka DVD +/-RW wraz z oprogramowaniem do nagrywania płyt Czytnik kart multimedialnych
Funkcjonalność BIOS	Zgodność ze specyfikacją UEFl Możliwość - skonfigurowania hasła „Power On”, - ustawienia hasła dostępu do BIOSu (administratora), - blokady portów USB, COM - wyłączenia portów USB; - wyłączenia portu szeregowego; - kontroli sekwencji boot-owania; - blokowania startu systemu z urządzenia USB
Funkcjonalność obudowy	- konstrukcja pozwalająca na beznarzędziowy dostęp do komponentów (kart rozszerzeń, napędów) - minimalna ilość wnęk. 2x 5,25” zewnętrzne, 2x 3,5” wewnętrzne - zasilacz o mocy min. 320W i skuteczności min. 90%, z aktywnym filtrem PFC - Głośność jednostki centralnej mierzoną zgodnie z normą ISO 7779 oraz wykazaną zgodnie z normą ISO 9296 w pozycji operatora w trybie jałowym (IDLE) wynoszącą maksymalnie 28 dB

	(załączyć oświadczenie Wykonawcy potwierdzające zmierzoną wg wymagań Zamawiającego głośność)
Oprogramowanie	- System operacyjny klasy PC nie wymagający aktywacji za pomocą telefonu lub Internetu, spełniający następujące wymagania poprzez natywne dla niego mechanizmy, bez użycia dodatkowych aplikacji: • Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek; • Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu; • Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW; • Internetowa aktualizacja zapewniona w języku polskim; • Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; • Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe; • Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi) • Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer • Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta. • Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. • Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. • Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych. • Funkcje związane z obsługą komputerów typu TABLET PC, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego. • Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika. • Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. • Wbudowany system pomocy w języku polskim; • Certyfikat producenta oprogramowania na dostarczany sprzęt; • Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); • Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; • Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509; • Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji; • System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; • Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach; • Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń; • Graficzne środowisko instalacji i konfiguracji; • Transakcyjny system plików pozwalający na stosowanie przydziałów na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe; • Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki,

	modemy, woluminy dyskowe, usługi katalogowe • Udostępnianie modemu; • Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej; • Możliwość przywracania plików systemowych; • System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.) • Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np przy użyciu numerów identyfikacyjnych sprzętu). • Koszt połączenia do telefonicznego serwisu technicznego powinien być równoważny co najwyżej połączeniu lokalnemu (inaczej: linii 0-801; preferencja: 0-800, linia bezpłatna dla użytkownika końcowego); • Telefoniczne wsparcie techniczne w języku polskim w dni robocze od 8:00 do 17:00 zapewniony przez producenta lub dostawcę co najmniej przez 5 lat od chwili zakupu - Pakiet biurowy zawierający min. edytor tekstów, arkusz kalkulacyjny, edytor prezentacji oraz program do tworzenia i zarządzania bazami danych. - Pakiet antywirusowy z subskrypcją baz szczepionek przez okres 3 lat spełniający wymagania minimalne określone w pkt. 5.6.2
Bezpieczeństwo	Komputer musi posiadać: - możliwość zastosowania zabezpieczenia fizycznego jednostki centralnej w postaci linki metalowej lub kłódki (oczko w obudowie do założenia kłódki) - zintegrowany z płytą główną 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)
Wymagania dodatkowe	Zintegrowane w obudowie: - Porty USB: min. 10 gniazd, w tym co najmniej 4 w standardzie USB 3.0, oraz 4 z przodu obudowy - Złącza video: : min. 1x D-Sub, 1x DisplayPort - Porty audio: z tyłu obudowy: wejście i wyjście liniowe, z przodu obudowy: wyjście na słuchawki, wejście na mikrofon - Gniazdo RS232, Gigabit Ethernet, 2x PS/2 Zintegrowane na płycie wolne sloty: min. 1 złącze PCI Express x16, 1 złącza PCI, 1 złącze PCI Express x1 Klawiatura w układzie polski programisty, Mysz laserowa z dwoma klawiszami oraz rolką (scroll) - zestaw płyt umożliwiający przywrócenie zainstalowanego systemu operacyjnego w wersji 32 i 64-bit
Certyfikaty i standardy	- Certyfikat ISO9001 oraz ISO14001 dla producenta sprzętu - EnergyStar 5.0 - Dokument potwierdzający poprawną współpracę oferowanych modeli komputerów z oferowanym systemem operacyjnym (należy załączyć do oferty np. wydruk ze strony www producenta oprogramowania) - Deklaracja zgodności CE
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
Monitor	
Typ ekranu	Ekran ciekłokrystaliczny z aktywną matrycą TFT 20”
Jasność	250 cd/m2
Kontrast	1000:1
Kąty widzenia (poziom/pion)	170/160 stopni
Czas reakcji matrycy	max 5ms

Rozdzielczość	min. 1600 x 900 przy 60Hz
Dostępna regulacja	wysokość monitora, kąt nachylenia ekranu, obrotowa podstawa, obrotowy ekran
Podświetlenie	LED
Bezpieczeństwo	Możliwość zastosowania zabezpieczenia fizycznego w postaci linki metalowej
Zużycie energii	22W (typowe); 30W (maksymalnie), 0,5W (czuwanie)
Złącze	min. D-Sub, DisplayPort , 2x USB
Certyfikaty i standardy	- Energy Star 5.0 - Certyfikat ISO9001 oraz ISO14001 dla producenta sprzętu - Deklaracja zgodności CE
Inne	Głośniki stereo, zdejmowalna podstawa, otwory montażowe w obudowie w celu instalacji naściennej
Gwarancja (komputer z monitorem)	5 lat gwarancji świadczonej w miejscu eksploatacji sprzętu - czas reakcji serwisu: do końca następnego dnia roboczego - w przypadku awarii komputerowych dysków twardych - dysk uszkodzony pozostaje u Zamawiającego

5.6 Dostawa, instalacja sprzętu komputerowego i oprogramowania

Wykonawca jest zobowiązany do skalkulowania wszelkich kosztów związanych z:
- zakupem sprzętu komputerowego i oprogramowania (licencje na oprogramowanie powinny zapewnić Zamawiającemu możliwość wielokrotnego użyczania sprzętu komputerowego wraz z oprogramowaniem dla BO o ile jest to wymagane przez producentów oprogramowania),
- dostawą i instalacją sprzętu w docelowym miejscu eksploatacji u BO .
- podłączeniem i uruchomieniem połączeń do węzłów dostępowych dla dostarczonych urządzeń, w ramach wybudowanej infrastruktury
- oznakowaniem przedmiotu zamówienia zgodnie z zgodnie z wytycznymi Władzy Wdrażającej zawartymi w „Przewodniku w zakresie promocji projektów finansowanych w ramach Programu Operacyjnego Innowacyjna Gospodarka, 2007- 2013”
- świadczeniem usług gwarancyjnych i serwisowych dla dostarczonych urządzeń na warunkach określonych w SIWZ
- świadczeniem wsparcia technicznego dla dostarczonego oprogramowania i sprzętu komputerowego.

5.6.1 Dostawa zestawów komputerowych wraz z podstawowym oprogramowaniem z przeznaczeniem dla beneficjentów ostatecznych – 80 kpl

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
Komputer typu All-in-One przeznaczony do zapewnienia beneficjentowi ostatecznemu dostępu do sieci Internet, dedykowany do obsługi aplikacji biurowych, poczty elektronicznej, grafiki prezentacyjnej, multimediów i nauczania na odległość		
1	Ekran	Przekątna: 20 cali Rozdzielczość: HD+ (1600x900) TN, Podświetlenie LED, Jasność: 250 cd/m2, Format 16:9. Kontrast 1000:1, Czas reakcji matrycy 5 ms, Kąty widzenia: 170/160 stopni
2	Procesor	Procesor musi osiągać wydajność, przy nominalnych parametrach pracy procesora określonych przez jego producenta, na poziomie 4970 pkt w teście PassMark CPU Mark (wynik zaproponowanego procesora musi znajdować się na stronie http://www.cpubenchmark.net, z której wydruk należy dołączyć do oferty)

		Procesor musi obsługiwać 64-bitowe systemy operacyjne.
3	Pamięć RAM	4 GB z możliwością rozszerzenia do 16 GB Ilość banków pamięci: min. 2 szt. Ilość wolnych banków pamięci: min. 1 szt.
4	Dysk twardy	500 GB
5	Karta graficzna	Zintegrowana z procesorem lub zewnętrzna
6	Karta dźwiękowa	Zintegrowana z płyta główną
7	Karta sieciowa	WiFi 802.11b/g/n, Bluetooth 4.0, LAN 10/100/1000 Mbit/s
8	Porty	Wbudowane wyjście VGA, 6 x USB w tym min 2 x USB 3.0 na bocznym panelu obudowy , 1 x RJ 45 (LAN), 1 x wyjście na słuchawki, 1 x wejście na mikrofon, RS-232, PS/2, Mini PCI Express, czytnik kart 11w1. Wymagana ilość portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.
9	Klawiatura	Klawiatura w układzie polski programisty – w kolorze zbliżonym do koloru obudowy, min 104 klawisze
10	Mysz	Mysz (scroll) w kolorze zbliżonym do koloru obudowy
11	Napęd optyczny	Nagrywarka DVD +/-RW wraz z dołączonym oprogramowaniem do odtwarzania i nagrywania
12	Obudowa	- zintegrowana z monitorem (AIO) – stopa musi umożliwiać regulację w pionie (min 110mm), poziomie (+/- 45stopni) oraz odchylenie (Tilt:10 stopni do 25 stopni) – musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) lub kłódki (oczko w obudowie do założenia kłódki) – zainstalowany fabrycznie czujnik otwarcia obudowy – Możliwość zainstalowania komputera na ścianie przy wykorzystaniu ściennego systemu montażowego VESA – Wbudowane w obudowę przyciski sterowania głośnością – wbudowane głośniki 2 x 2W skierowane w stronę operatora – dołączony nośnik ze sterownikami – Suma wymiarów nie może przekraczać (razem ze stopą): 1200 mm
13	Kamera	Zintegrowana z obudową, o rozdzielczości 1 Mpix z mechaniczną przesłona obiektywu
14	Bezpieczeństwo	TPM w wersji 1.2
15	Waga	Maksymalnie 9 kg
16	Moc	Maksymalnie 150 W, sprawność minimum 85%
17	Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji operatora w trybie IDLE wynosząca maksymalnie 23 dB . (załączyć oświadczenie Wykonawcy potwierdzające zmierzoną wg wymagań Zamawiającego głośność)
18	BIOS	- Możliwość odczytania z BIOS: o Modelu komputera, numeru seryjnego, o Daty wydania oraz wersji BIOS, o Modelu procesora wraz z informacjami o ilości rdzeni, o Informacji o ilości pamięci RAM, o Informacji o dysku twardym (model), o Informacji o napędzie optycznym (model), - Możliwość selektywnego (pojedynczego) blokowania portów USB z poziomu BIOS

		- Możliwość bootowania systemu z czytnika kart - Możliwość ustawienia portów USB, sieci, napędu DVD w tryb „no-boot” - Możliwość wyłączenia kamery zintegrowanej, czytnika kary, - Możliwość wyłączenia urządzeń podłączonych poprzez porty SATA I i SATA II - Możliwość wyłączenia przycisków na przedniej obudowie, - Obsługa BIOS za pomocą klawiatury oraz myszy
19	Zainstalowane oprogramowanie	Zainstalowany system operacyjny, wraz z nośnikiem, nie wymagający aktywacji za pomocą telefonu lub internetu, musi spełniać następujące wymagania, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: • Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym polskim i angielskim, • Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika. • Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne, • Możliwość dokonywania aktualizacji poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego, • Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego, • Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; • Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami, • Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe, • Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim, • Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi), • Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer, • Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji, • Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji, • Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe, • Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. • Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, • Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. • Wbudowany system pomocy w języku polskim; • Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); • Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; • Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509; • Mechanizmy logowania w oparciu o: 1) Login i hasło,

		2) Karty z certyfikatami (smartcard), 3) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), • Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu, • Wsparcie dla algorytmów Suite B (RFC 4869), • Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; • Wsparcie dla środowisk Java i .NET Framework 1.1 i 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach, • Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń, • Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem, • Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową, • Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację, • Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe, • Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe • Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej, • Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci, • Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.), • Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu), • Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie min. 4 maszyn wirtualnych, • Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika, • Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów „w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB. • Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych • Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych. • Możliwość nieodpłatnego instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu. • Możliwość downgarde'u do wcześniejszej wersji - Zainstalowane oprogramowanie biurowe - kompletny pakiet oprogramowania biurowego z edytorem tekstu, arkuszem kalkulacyjnym, oprogramowaniem bazodanowym i oprogramowaniem do tworzenia prezentacji. - Pakiet antywirusowy z subskrypcją baz szczepionek przez okres 3 lat określony w pkt. 5.6.2

20	Dodatkowe oprogramowanie	- Oprogramowanie umożliwiające aktualizacje zainstalowanego oprogramowania oraz skanowanie dysku z poziomu podsystemu bezpieczeństwa (nie systemu operacyjnego). - Możliwość dostępu do Internetu z poziomu w/w podsystemu. - Oprogramowanie służące do obsługi napędu DVD. - Oprogramowanie umożliwiające aktualizacje sterowników oraz podsystemu zabezpieczeń poprzez Internet. - Oprogramowanie umożliwiające wykonanie kopii bezpieczeństwa systemu operacyjnego i danych użytkownika na dysku twardym, zewnętrznych dyskach, oraz ich odtworzenie po awarii systemu operacyjnego bez potrzeby jego reinstalacji. Oprogramowanie w wersji polskiej lub angielskiej - Możliwość monitorowania na poziomie sprzętu poprzez mechanizm watchdog pracy co najmniej jednego programu np. programu antywirusowego. W przypadku wykrycia braku działania monitorowanego programu narzędzie zarządzające musi wysyłać alert w postaci wiadomości email na wybrany komputer np. administratora - Możliwość sprzętowego uruchamiania komputera (ze stanu pełnego wyłączenia - soft off S5) o zadanej godzinie. - Przechowywanie logów wykonanych operacji z możliwością ich zdalnego przeglądania przez administratora - Możliwość zdalnego przejęcia konsoli graficznej systemu operacyjnego - Możliwość zdalnego zablokowania obsługi urządzeń dołączanych do portów USB
21	Certyfikaty i normy	- Certyfikat ISO9001 oraz ISO14001 dla producenta sprzętu - EnergyStar 5.0 - Deklaracja zgodności CE - Dokument potwierdzający poprawną współpracę oferowanych modeli komputerów z oferowanym systemem operacyjnym (należy załączyć do oferty np. wydruk ze strony www producenta oprogramowania) Zamawiający wymaga, aby dokumenty potwierdzające oraz wyniki testów były sporządzone w języku polskim bądź w innym języku z przetłumaczeniem na język polski
22	Wsparcie techniczne producenta ,inne wymagania	-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 - Wykonawca zobowiązany jest dostarczyć wraz z ofertą kartę produktową oferowanego zestawu umożliwiającą weryfikację parametrów oferowanego sprzętu
23	Gwarancja	5-letnia gwarancja świadczona na miejscu u klienta. Czas reakcji serwisu - do końca następnego dnia roboczego. Serwis gwarancyjny urządzeń musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta – wymagane jest oświadczenie Wykonawcy potwierdzające, że serwis będzie realizowany przez Producenta lub autoryzowanego Partnera Serwisowego producenta (oświadczenie Wykonawcy należy dołączyć do oferty).
24	Akcesoria dodatkowe	Listwa zasilająca : Liczba gniazd wyjściowych: 5 szt., długość przewodu zasilającego: min. 1,8 metra, napięcie znamionowe: 230 V AC, prąd znamionowy: 10 A, częstotliwość: 50 Hz,, bezpiecznik nadprądowy

5.6.2 Oprogramowanie antywirusowe oraz antyspyware .

Wymagania minimalne względem oprogramowania antywirusowego
Pełne wsparcie dla systemów operacyjnych oferowanych przez Wykonawcę w komputerach stacjonarnych i przenośnych (w wersji 32 i 64-bit) Wersja programu dostępna zarówno języku polskim jak i angielskim. Pomoc w programie (help) w języku polskim. Dokumentacja do programu dostępna w języku polskim. 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. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 5. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 6. 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. 7. 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). 8. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 9. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. 10. Aplikacja musi umożliwiać automatyczne uruchomienie skanowania w momencie wykrycia bezczynności systemu 11. Bezczynność systemu musi być wykrywana co najmniej w oparciu o aktywny wygaszacz ekranu, blokadę komputera, wylogowanie użytkownika 12. Możliwość skanowania dysków sieciowych i dysków przenośnych. 13. Skanowanie plików spakowanych i skompresowanych. 14. Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (w tym z uwzględnieniem plików bez rozszerzeń). 15. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 16. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. 17. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu. 18. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera. 19. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji. 20. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. 21. 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. 22. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird (w wersji 5.x lub starszej) i Windows Live Mail. Funkcje programu dostępne są bezpośrednio z menu programu pocztowego. 23. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird (w wersji 5.x lub starszej) i Windows Live Mail. 24. 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).

25. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
26. Możliwość definiowania różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie.
27. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
28. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
29. Blokowanie możliwości przeglądania wybranych stron internetowych. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony.
30. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez użytkownika.
31. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
32. Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie.
33. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
34. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
35. Użytkownik ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
36. Aplikacja 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. Interfejs programu ma oferować funkcję pracy w trybie bez grafiki gdzie cały interfejs wyświetlany jest w formie formatek i tekstu.
47. Interfejs programu ma mieć możliwość automatycznego aktywowania trybu bez grafiki w momencie, gdy użytkownik przełączy system Windows w tryb małej ilości kolorów (256).
48. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.
49. 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.
50. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji musi być takie

samo.

51. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.
52. 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.
53. 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.
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 ma umożliwiać użytkownikowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, płyt CD/DVD i pamięci masowych FireWire.
57. 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.
58. Aplikacja musi posiadać funkcjonalność, która automatycznie uzupełni elementy wymagane dla tworzenia reguł w oparciu o informacje dostępne z aktualnie podłączonego nośnika.
59. 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.
60. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
61. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
62. Użytkownik ma posiadać możliwość takiej konfiguracji aplikacji aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.
63. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
64. Moduł HIPS musi posiadać możliwość pracy w jednym z czterech trybów:
    - tryb automatyczny z regułami gdzie aplikacja automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    - tryb interaktywny, w którym to aplikacja 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 aplikacja uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu aplikacja musi samoczynnie przełączyć się w tryb pracy oparty na regułach.
65. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
66. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
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. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
73. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym.

74. W momencie wykrycia trybu pełno ekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się harmonogramie zadań aplikacji.
75. Użytkownik ma mieć możliwość skonfigurowania programu tak aby automatycznie aplikacja włączała powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym po określonym przez użytkownika czasie.
76. Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania.
77. Aplikacja musi posiadać opcję która umożliwi zgłoszenie podejrzanej witryny phishingowej bezpośrednio do laboratorium producenta
78. Aplikacja musi posiadać funkcję, która automatycznie powiadomi o dostępnej, nowszej wersji oprogramowania.
79. Po zainstalowaniu aplikacji wymagane jest wstępne skanowanie komputera.
80. Oprogramowanie musi posiadać zaawansowany skaner pamięci, który pozwala na wykrywanie i blokowanie zagrożeń, ukrytych w zmodyfikowanych aplikacjach
81. Program musi posiadać funkcję blokowania zagrożeń, które ukierunkowane są na luki (exploity) w aplikacjach takich jak m. in. przeglądarki internetowe, klienci pocztowi, czytniki PDF, itp.
82. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

Zabezpieczenie portali społecznościowych

83. Aplikacja musi posiadać możliwość uruchomienia skanera zawartości profil użytkownika na portalu Facebook.
84. Skaner musi posiadać możliwość skanowania obiektów znajdujących się na tablicach znajomych użytkownika.
85. Skaner musi mieć możliwość dodania ostrzeżenia pod zarażonymi lub podejrzanymi obiektami.
86. Skaner musi posiadać możliwość automatycznego skanowania dodawanych obiektów oraz możliwość uruchomienia skanowania na żądanie.
87. Skaner musi posiadać możliwość uruchomienie skanera antywirusowego online bezpośrednio z poziomu interfejsu aplikacji Facebook'a.
88. Skaner musi posiadać możliwość gromadzenia statystyk skanowania profili.
89. Aplikacja musi posiadać możliwość powiadomienia użytkownika poprzez wiadomość e-mail o zagrożeniach wykrytych podczas procesu automatycznego skanowania zawartości profilu.
90. Aplikacja musi posiadać możliwość publikacji statystyk odnośnie liczby wykonanych skanowań oraz wykrytych zagrożeń na ścianie użytkownika.

5.7 Usługi wsparcia technicznego i serwisu gwarancyjnego systemu.

(sprzętu komputerowego oraz sieci szerokopasmowej)

5.7.1 Wsparcie techniczne i obsługa serwisowa zestawów komputerowych i oprogramowania .

Zamawiający wymaga, aby oferowane zestawy komputerowe dostarczone w ramach realizacji umowy posiadały świadczenia gwarancyjne realizowane przez Wykonawcę.

Minimalne warunki świadczenia usług :

- 5-letnia gwarancja na bazie gwarancji producenta , oficjalnego dystrybutora lub importera sprzętu liczona od dnia podpisania protokołu odbioru końcowego zestawów komputerowych, świadczona na miejscu u BO potwierdzona kartą gwarancyjną.
- przyjmowanie zgłoszeń serwisowych w godz. 08.00 – 20.00, w dni robocze poprzez wydzielony telefon serwisowy, fax ,e-mail
- czas reakcji serwisu - do końca następnego dnia roboczego
- świadczenia usług wsparcia technicznego w zakresie sprzętu i oprogramowania

dostarczonego w ramach zamówienie poprzez określenie wydzielonego nr telefonu serwisowego
- usunięcie usterki w ciągu najpóźniej 3 dni roboczych od momentu zgłoszenia
- usunięcie awarii w ciągu najpóźniej 2 dni roboczych od momentu zgłoszenia
- w przypadku braku możliwości naprawy w miejscu użytkowania sprzętu, wykonawca zobowiązuje się zapewnić na czas naprawy sprzęt zastępczy o parametrach nie gorszych niż sprzęt zabrany do naprawy
- w przypadku awarii dysków twardych i braku możliwości ich naprawy uszkodzony dysk pozostaje u Zamawiającego.

Inne wymagania wobec Wykonawcy :

- Gwarant udostępnia Zamawiającemu BIOS, firmware i sterowniki na płytach CD. Dodatkowo Zamawiający i Beneficjenci ostateczni będą mieli dostęp do aktualnych sterowników poprzez wskazaną przez Wykonawcę stronę internetową.
- Gwarant ponosi koszty napraw gwarancyjnych (serwisowych), włączając w to koszt części. W przypadku, gdy naprawy nie uda się zrealizować w siedzibie BO , Gwarant ponosi również koszty transportu.
- dokonywania przeglądów okresowych sprzętu, co najmniej jednego przeglądu na 2 lata obejmującego diagnostykę oraz konserwację sprzętu.
- prowadzenie bazy napraw z możliwością dostępu on-line przedstawiciela Zamawiającego.

5.7.2. Serwis gwarancyjny i utrzymanie infrastruktury sieci szerokopasmowej

Zamawiający wymaga, aby oferowany sprzęt do budowy sieci szerokopasmowej dostarczony w ramach realizacji umowy posiadał świadczenia gwarancyjne oraz wsparcie techniczne realizowane przez Wykonawcę

Minimalne warunki świadczenia oraz zakres usług :

a)3-letnia gwarancja Wykonawcy liczona od dnia podpisania protokołu odbioru końcowego sieci szerokopasmowej , świadczona na miejscu budowy.

b)bieżące monitorowanie infrastruktury i wykrywanie awarii oraz ich usuwanie (w ciągu maksymalnie 24 godzin), a w przypadku kiedy dotyczą uszkodzeń i awarii urządzeń sieciowych objętych gwarancją, obsługa procedur gwarancyjno-serwisowych

c) w przypadku braku możliwości naprawy lub usunięcia awarii w ciągu 24 godzin, zapewnienie urządzeń zastępczych na czas naprawy w celu zachowania ciągłości pracy sieci;

d) sporządzanie okresowych raportów obciążenia infrastruktury sieciowej

e) aktualizacja oprogramowania urządzeń transmisyjnych ,sieciowych, w tym aktualizacja firmware'ów, oraz wykonywanie update'ów systemu bezpieczeństwa – zgodnie z zaleceniami producenta urządzeń.

f) dokonywanie przeglądów okresowych infrastruktury aktywnej, co najmniej jednego przeglądu w roku obejmującego diagnostykę oraz konserwację sprzętu.

g) dokonywanie przeglądów okresowych infrastruktury pasywnej (maszty , wieże , okablowanie) co najmniej jednego przeglądu na 2 lata ,obejmującego sprawdzenie ich stanu oraz konserwację

VI. OGÓLNE WARUNKI WYKONANIA I ODBIORU ROBÓT

1. Pozostałe wymagania od Wykonawców

Poza robotami podstawowymi, opisanymi w dokumentacji przetargowej wykonawca jest zobowiązany do skalkulowania wszelkich robót pomocniczych, jakie uzna za niezbędne do prawidłowego wykonania robót dla przyjętej technologii , uwzględniając warunki ich wykonania.
Wykonawca powinien ponadto uwzględnić w cenie – w ramach kosztów dodatkowych – wszelkie pozostałe koszty związane z kompleksową realizacją zamówienia, w tym:

- koszty opracowania planu bezpieczeństwa i ochrony zdrowia oraz wykonania jego zaleceń,
- koszty zużycia mediów niezbędnych na czas budowy,
- koszty zabezpieczenia istniejących elementów obiektu oraz wyposażenia (urządzeń) Użytkownika przed ich zniszczeniem w trakcie wykonywania robót,
- koszty związane z zorganizowaniem pracy w sposób minimalizujący zakłócenie prowadzenia bieżącej działalności Użytkownika,
- koszty urządzenia placu budowy,
- koszty oznakowania robót i zabezpieczenia warunków bhp i ppoż. w trakcie realizacji robót,
- koszty płatnych prób, badań, odbiorów technicznych, zgodnie z wymogami odpowiednich instytucji,
- koszty opracowania dokumentacji powykonawczej,
- koszty uporządkowania oraz przywrócenia obiektu oraz terenu po wykonanych robotach do stanu pierwotnego wraz z naprawą ewentualnych szkód użytkownikowi lub osobom trzecim,
- wszelkie inne koszty wynikłe z analizy dokumentacji projektowej, przyjętej przez Wykonawcę technologii wykonania inwestycji oraz dokonanej wizytacji terenu budowy.

2. Szkolenia dla administratorów sieci

W ramach robót wymagane jest aby Wykonawca sieci przeprowadził szkolenia dla wyznaczonych pracowników Zamawiającego (którzy będą pełnić role osób monitorujących sieć internetową) w zakresie:
- Konfiguracji i zarządzania radioliniami
- Podstawowej konfiguracji i zarządzania urządzeniami aktywnymi sieci
- Administracja i zarządzanie bezprzewodowa siecią WLAN (kontroler sieci bezprzewodowej)
- Zarządzania systemem LMS
- Polityki autentykacji i autoryzacji użytkowników sieci
- Wykonywania kopii bezpieczeństwa, plików konfiguracyjnych itp.

3. Dokumenty odbioru końcowego

- Dzienniki budowy (jeśli będzie wymagany)
- Oświadczenie kierownika budowy o zgodności wykonania obiektu budowlanego z projektem budowlanym i warunkami pozwolenia na budowę, przepisami i obowiązującymi Polskimi Normami.
- Dokumentacja techniczna powykonawcza
- Protokoły odbiorów częściowych
- Protokoły z pomiarów i testów urządzeń transmisyjnych oraz całej sieci radiowej,
- Odpowiednie atesty i certyfikaty
- Instrukcje obsługi, dokumentacje i inne dokumenty dostarczane wraz ze sprzętem, przez producenta

VII. CZĘŚĆ INFORMACYJNA PROGRAMU

7.1 Akty prawne i rozporządzenia

Zamówienie winno zostać wykonane zgodnie z następującymi aktami prawnymi, w szczególności :

1.1 Ustawa z dnia 7 lipca 1994r. Prawo Budowlane (Dz. U. z 2010 Nr 243 poz. 1623 ze zm.) oraz wydanych na jej podstawie rozporządzeń,

1.2 Ustawa z dnia 16 lipca 2004r. Prawo Telekomunikacyjne (Dz. U. z 2004r. Nr 171, poz. zm.) oraz wydanych na jej podstawie rozporządzeń,

1.3 Ustawa z dnia 27 kwietnia 2001r. Prawo Ochrony Środowiska (Dz. U. z 2006r. Nr 129, poz. 902 ze zm.) oraz wydanych na jej podstawie rozporządzeń,

1.4 Rozporządzenia Ministra Infrastruktury z dnia 2 września 2004 roku w sprawie szczegółowego zakresu i formy dokumentacji projektowej, specyfikacji technicznych wykonania i odbioru robót budowlanych oraz programu funkcjonalno- użytkowego (Dz. U. z 2004r. Nr 202, poz. 2072 ze zm.),

1.5 Ustawa o wspieraniu rozwoju usług i sieci telekomunikacyjnych Dz. U. nr 106 z dnia 16 czerwca 2010 r. , poz. 675

1.6 „Ustawa o świadczeniu usług droga elektroniczna z dnia 18 lipca 2002 roku"

1.7 „Ustawa o dostępie warunkowym"

1.8 „Ustawie z dnia 18 września 2001 r. o podpisie elektronicznym".

1.9 „Ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne z dnia 17 lutego 2005 roku".

1.10 Rozporządzenie Rady Ministrów z dnia 9 listopada 2004 r. w sprawie określenia rodzajów przedsięwzięć mogących znacząco oddziaływać na środowisko oraz szczegółowych uwarunkowań związanych z kwalifikowaniem przedsięwzięcia do sporządzenia raportu o oddziaływaniu na środowisko (Dz. U. z dnia 3 grudnia 2004 r.)

1.11 Rozporządzenie Ministra Infrastruktury z dnia 26 października 2005r. w sprawie warunków technicznych jakim powinny odpowiadać telekomunikacyjne obiekty budowlane i ich usytuowanie (Dz. U. z 2005r. Nr 219, poz. 1864),

1.12 Rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 roku w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych,

1.13 Rozporządzenie Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych

1.14 Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych

1.15 Uchwała Sejmu Rzeczypospolitej Polskiej z dnia 14 lipca 2000 r. w sprawie budowania podstaw społeczeństwa informacyjnego w Polsce.

<u>Ramy prawne Komisji Europejskiej w sektorze komunikacji elektronicznej</u>

a. Dyrektywa (2002/19/EC) z dnia 7 marca 2002r. w sprawie dostępu do sieci łączności elektronicznej i urządzeń towarzyszących oraz ich łączenia (Dz. Urz. WE L. 108 z 24 kwietnia 2002r.);
b. Dyrektywa (2002/20/EC) z dnia 7 marca 2002 r. w sprawie zezwoleń na udostępnianie sieci i usługi łączności elektronicznej (Dz. Urz. WE L. 108 z 24 kwietnia 2002r.);
c. Dyrektywa (2002/21/EC) z dnia 7 marca 2002r. w sprawie jednolitej struktury regulacji dla sieci i usług komunikacji elektronicznej (DZ. Urz. WE L. 108 z 24 kwietnia 2002r.);
d. Dyrektywa (2002/22/EC) z dnia 7 marca 2002r. w sprawie usługi powszechnej i praw użytkowników odnoszących się do sieci i usług łączności elektronicznej (Dz. Urz. WE L. 108 z 24 kwietnia 2002r.) ;
e. Dyrektywa (2002/58/EC) z dnia 12 lipca 2002r. w sprawie przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (Dz. Urz. WE L. 201 z 31 lipca 2002r.);
f. Dyrektywa (2002/77/EC) z dnia 16 września 2002r. w sprawie konkurencji na rynkach sieci i usług łączności elektronicznej (Dz. Urz. WE L. 249 z 17 września 2002r.);
g. Rozporządzenie (EC) 2887/2000 o niezależnym dostępie do pętli lokalnych

Przy projektowaniu i budowie sieci radiowej należy wziąć pod uwagę następujące normy i rekomendacje komitetu ITU:

3.1 Recommendation ITU-R 838, Specific Attenuation Model For Rain For Use In Prediction Methods

3.2 Rekomendacja (zalecenie) ITU-R P.838-3: „Ścisły (specyficzny) model do zastosowania w metodach przewidywania tłumienia przez deszcz”

3.3 Recommendation ITU-R P.676-3, Attenuation By Atmospheric Gases - Rekomendacja (zalecenie) ITU-R P676.3: „Tłumienie przez gazy atmosferyczne”

3.4 Recommendation ITU-R Pn 837-1, Characteristics Of Precipitation For Propagation Modelling – Rekomendacja (zalecenie) ITU-R PN 837-1: „Charakterystyki opadów atmosferycznych dla modelowania propagacji”

3.5 Recommendation ITU-R P.530-7, Propagation Data And Prediction Methods Required For The Design Of Terrestrial Line-Of-Sightsystems - Rekomendacja (zalecenie) ITU-PN P530-7: „Dane propagacyjne i metody przewidywania wymagane dla projektowania systemów naziemnych z linią bezpośredniej widzialności”