Projekt współfinansowany przez Unię Europejską z Europejskiego

Funduszu Rozwoju Regionalnego w ramach

Programu Operacyjnego Innowacyjna Gospodarka



PROGRAM FUNKCJONALNO - UŻYTKOWY

W zakresie zadania inwestycyjnego pn.

**„Przeciwdziałanie wykluczeniu cyfrowemu**

**na terenie Gminy Bojanów”**

Opis przedmiotu zamówienia wg Wspólnego Słownika Zamówień (CPV):

324 18000-6 (sieć radiowa)

453 12330-9 (montaż anten radiowych)

324 13100-2 (routery sieciowe)

324 15000-5 (sieć ethernet)

324 12110-8 (sieć internetowa)

323 44210-1 (sprzęt radiowy)

324 20000-3 (urządzenia sieciowe)

324 21000-0 (okablowanie sieciowe)

324 22000-7 (elementy składowe sieci)

453 15600-4 (instalacja niskiego napięcia)

453 10000-3 (roboty instalacyjne elektryczne)

453 11000-0 (roboty w zakresie okablowania oraz instalacji elektrycznych)

454 53000-7 (roboty remontowe i renowacyjne)

724 00000-4 (usługi internetowe)

302 13100-6 (komputery przenośne)

727 20000-3 (usługi w zakresie rozległej sieci komputerowej)

726 11000-6 (usługi w zakresie wsparcia technicznego)

805 000 00-9 (usługi szkoleniowe)

805 331 00-0 (usługi szkolenia komputerowego)

**ZAMAWIAJĄCY:**

**Gmina Bojanów**  
ul. Parkowa 5  
37-433 Bojanów

Zawartość:

1. Część opisowa programu
2. Ogólne wymagania zamawiającego
3. Aktualne uwarunkowania przedmiotu zamówienia
4. Ogólne właściwości funkcjonalno-użytkowe
5. Szczegółowe właściwości i wymagania funkcjonalno-użytkowe
6. W zakresie przygotowania dokumentacji projektowej, harmonogramu prac oraz pozostałej niezbędnej dokumentacji
7. W zakresie budowy masztów antenowych oraz konstrukcji wsporczych pod anteny (elementy pasywne)
8. W zakresie budowy sieci szkieletowej i stacji bazowych
9. W zakresie budowy węzłów dystrybucyjnych
10. W zakresie budowy warstwy dostępowej
11. W zakresie budowy Głównego Węzła Dystrybucyjnego i Centrum Zarządzania siecią Gminy
12. W zakresie dostawy i instalacji sprzętu komputerowego i oprogramowania
13. W zakresie usługi administrowania i serwisowania systemu (sprzętu komputerowego oraz sieci szerokopasmowej)
14. W zakresie zapewnienia usługi dostępu do Internetu dla Beneficjentów ostatecznych
15. W zakresie organizacji szkoleń z podstaw obsługi komputera, pakietu biurowego, oraz obsługi Internetu
16. Ogólne warunki wykonania i odbioru robót
17. Część informacyjna programu
18. **CZĘŚĆ OPISOWA PROGRAMU**

Przedmiotem zamówienia jest kompleksowa realizacja zadania pn. „Przeciwdziałanie wykluczeniu cyfrowemu na terenie Gminy Bojanów”

Zakres projektu składa się następujących zadań:

1. **Przygotowania dokumentacji projektowej, harmonogramu prac oraz innej niezbędnej dokumentacji**

- Opracowanie projektów budowlanych w zakresie budowy 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

- Inne konieczne dokumenty

1. **Budowy masztów antenowych oraz konstrukcji wsporczych pod anteny**

- Budowa masztów antenowych w miejscowościach: (Bojanów, Cisów Las, Gwoźdźce, Stany, Maziarnia)

- Instalacja szaf zewnętrznych (typu outdoor) oraz wykonanie instalacji okablowania sygnałowego pod potrzeby instalacji anten

1. **Budowy sieci szkieletowej w oparciu o radiolinie cyfrowe i stacji bazowych WiMAX**

- Dostawa, instalacja oraz konfiguracja radiolinii cyfrowych

- Dostawa, instalacja oraz konfiguracja stacji bazowych WiMAX

1. **Budowy Węzłów Dystrybucyjnych**

- Dostawa, instalacja i konfiguracja elementów oraz urządzeń stanowiących wyposażenie Węzłów Dystrybucyjnych

- Dostawa, instalacja i konfiguracja przełączników sieciowych oraz UPSów

- Montaż szaf, uchwytów antenowych oraz przygotowanie infrastruktury kablowej w obiektach Węzłów Dystrybucyjnych

1. **Budowy warstwy dostępowej**

- Dostawa, instalacja i konfiguracja bezprzewodowych punktów dostępowych

- Dostawa i instalacja i konfiguracja urządzeń odbiorczych dla 100 Beneficjentów końcowych

1. **Wyposażenia Głównego Węzła Dystrybucyjnego i Centrum Zarządzania siecią szerokopasmową.**

- Adaptacja pomieszczenia przeznaczonego na Centrum Zarządzania

- Dostawa, instalacja oraz konfiguracja urządzeń i elementów do budowy Głównego Węzła Dystrybucyjnego (GWD) oraz Centrum Zarządzania siecią (przełącznika szkieletowego, kontrolera sieci bezprzewodowej, urządzenia bezpieczeństwa, serwerów oraz implementacja systemów do zarządzania użytkownikami i usługami sieci)

1. **Dostawy i instalacji sprzętu komputerowego i oprogramowania**

- Dostawa 40 szt. zestawów komputerowych wraz z oprogramowaniem

1. **Usługi serwisowania i administrowania siecią szerokopasmową oraz serwis i utrzymanie sprzętu komputerowego przez okres 36 miesięcy**
2. **Zapewnienie usługi dostępu do Internetu dla 100 gospodarstw domowych oraz 20 jednostek podległych przez okres 36 miesięcy.**
3. **Szkolenia z podstaw obsługi komputera (systemu operacyjnego, pakietu biurowego oraz Internetu).**

Niniejszy program na celu umożliwienie dokonania wyboru najkorzystniejszej oferty na opracowanie dokumentacji projektowej oraz budowy infrastruktury sieci szerokopasmowej Gminy Bojanów, a także dostawy sprzętu komputerowego, oprogramowania, jego serwisu i modernizacji a także organizacji szkoleń.  
Dokument zawiera opis zamierzenia inwestycyjnego pod kątem kryteriów funkcjonalnych, technicznych i jakościowych, oraz wskazuje technologie, które powinny być wykorzystane do budowy sieci – tak aby zapewnić optymalną relację ceny do jakości rozwiązania

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.

1. **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,

- 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.

1. Ogólne wymagania w zakresie usług i dostępności sieci

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

* Szybkość łącza Internetowego do użytkownika indywidualnego min: 1 Mb/s
* Szybkość łącza Internetowego od użytkownika indywidualnego min: 256 kbps
* Szybkość łącza Internetowego do użytkownika będącego jednostką podległą samorządowi terytorialnemu min 4 Mb/s
* Szybkość łącza Internetowego od użytkownika będącego jednostką podległą samorządowi terytorialnemu min 1 Mb/s
* Zapewnienie dostępności sieci na poziomie min. 96%
* Zapewnienie czasu usunięcia zgłoszonych usterek w czasie poniżej 24h
* Możliwość ustawienia strony www uruchamianej po zalogowaniu do systemu
* Możliwość blokowania wybranych stron www
* Możliwość blokady wybranych portów i usług (np. usług wymiany plików)

1. Ogólne wymagania w zakresie technologii sieci bezprzewodowej

Ponadto zrealizowany i uruchomiony dostęp do Internetu z wykorzystaniem sieci szerokopasmowej powinien spełnić następujące wymagania:

* Warstwa szkieletowa i dystrybucyjna sieci powinna być wykonana w oparciu o licencjonowane pasma radiowe (radiolinie, WiMAX) oraz połączenia dystrybucyjne punkt-punkt pracujące w nielicencjonowanym paśmie radiowym 5GHz
* sieć dostępowa powinna być wykonana i funkcjonować w oparciu o nielicencjonowane pasmo 2,4 GHz i 5 GHz z wykorzystaniem technologii MIMO
* węzły dostępowe winny być zamontowane na obiektach samorządowych
* wymagane jest aby do jednego bezprzewodowego punktu dostępowego 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 w warstwie dystrybucyjnej i dostępowej
* naziemna sieć bezprzewodowa powinna być zarządzana z Centrum Zarządzania, zlokalizowanego w budynku Urzędu Gminy w Bojanowie, i powinna zapewniać:
  + zarządzanie użytkownikami i usługami sieci
  + zarządzanie uszkodzeniami
  + zarządzanie konfiguracją
  + zarządzanie wydajnością
  + zarządzanie bezpieczeństwem
  + monitoring sieci
  + autentykację użytkowników
  + logowanie zdarzeń

W przypadku braku możliwości dostarczenia usługi dostępu do Internetu za pomocą sieci bezprzewodowej (naziemnej) lub dostarczenie takie byłoby nie efektywne ekonomicznie, dopuszczalne jest wykorzystanie innych technologii, np. sieci satelitarnej, pod warunkiem zapewnienia obydwu kanałów (odbieranie i wysyłanie).

W jednostkach podległych samorządowi terytorialnemu, zamawiający oczekuje podłączenia jednego łącza internetowego dla całego obiektu.

1. Ogólne wymagania w zakresie dokumentacji projektowej

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 2006r. Nr 156, poz. 1118 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 2006r. Nr 156, poz. 1118 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 całej Gminy Bojanów i powinna zwierać:

- projekty budowlane i projekty wykonawcze 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 centralnego węzła sieci z uwzględnieniem odpowiednich urządzeń (serwerów, urządzeń aktywnych routera dostępowego) 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.

1. **AKTUALNE UWARUNKOWANIA PRZEDMIOTU ZAMÓWIENIA**

Elementy na których będą instalowane, składniki projektu są obiektami mieszkalnymi, budynkami użyteczności publicznej oraz nieruchomościami należącymi do Gminy.

Nieruchomości, na których mają być zlokalizowane elementy projektu oraz ich okablowanie są własnością Zamawiającego.

Stacje robocze z dostępem do Internetu będą zlokalizowane w obiektach będących własnością zamawiającego, Wspólnot Mieszkaniowych, właścicieli i użytkowników wieczystych.

1. **OGÓLNE WŁAŚCIWOŚCI FUNKCJONALNO-UŻYTKOWE**

Zadaniem wykonawcy będzie zaprojektowanie, dostawa materiałów i urządzeń, wykonanie wszelkich prac budowlanych, montażowych i instalacyjnych oraz dostawa sprzętu komputerowego, serwis i usługa zapewnienia dostępu do Internetu dla tzw. Grupy Docelowej – w ramach projektu pn. „Przeciwdziałanie wykluczeniu cyfrowemu na terenie Gminy Bojanów”.

Zakres projektu będzie obejmował zatem budowę infrastruktury sieci szerokopasmowej. Najpierw zostanie zbudowany szkielet sieci oraz stacje bazowe (rdzeniowe węzły dystrybucyjne), na bazie którego powstanie warstwa dystrybucyjna (węzły dystrybucyjne), a następnie warstwa dostępowa (bezprzewodowe punkty dostępu). Końcowym etapem będzie wyposażenie Głównego Węzła Dystrybucyjnego oraz Centrum Zarządzania w sprzęt aktywny sieci oraz serwery usług- instalacja, konfiguracja i integracja systemu.

Sieć zostanie wykonana w oparciu o technologie bezprzewodowe, w oparciu o model hierarchiczny projektowania i budowy sieci, tzn. z podziałem na warstwę rdzenia, dystrybucji i dostępu.

Warstwa rdzeniowa

Warstwa rdzeniowa stanowi szkielet sieci. Szkielet sieci zostanie zbudowany w oparciu o Główny Węzeł Dystrybucji i Centrum Zarządzania siecią zlokalizowany w budynku Urzędu Gminy Bojanów oraz 4 Węzły Rdzeniowe zlokalizowane odpowiednio:

* WR1 – w miejscowości Bojanów
* WR2 – w miejscowości Maziarnia
* WR3 – w miejscowości Przyszów
* WR4 – w miejscowości Cisów Las

W ramach połączeń szkieletowych, lokalizacje WR zostaną połączone radioliniami cyfrowymi klasy operatorskiej o przepustowości min. 50 Mb/s FDD

Zadaniem warstwy rdzenia sieci jest zapewnienie wysokiej wydajności transmisyjnej (min. 50 Mb/s FDD) i dostępności połączeń szkieletowych dla Stacji Bazowych i połączeń dystrybucyjnych.

Ponadto w lokalizacji WR1 (w miejscowości Bojanów) zostanie zainstalowana Stacje Bazowa WiMAX o odpowiedniej konfiguracji, tak aby możliwe było połączenie wszystkich Jednostek Podległych na terenie miejscowości Bojanów.

Warstwa dystrybucyjna

Warstwa dystrybucyjne sieci zostanie zbudowana w oparciu o technologię WiMAX zgodnie ze standardem IEEE 802.16e.

Planowana jest instalacja min. 13 Węzłów Dystrybucyjnych (WD) zlokalizowanych w obiektach jednostek podległych Gminy (lista lokalizacji WD zamieszczona jest w dalszej części opracowania).

Zadaniem tej warstwy jest dostarczanie wysokiej jakości usług transmisji danych oraz dostępu do Internetu.

W ramach projektu planowane jest podłączenie wszystkich jednostek podległych Gminy Bojanów do warstwy dystrybucji, gdzie za pomocą mechanizmów QoS (Quality of Service) zachowana zostanie wysoka dostępność i jakość usług.

Ponadto warstwa dystrybucyjna będzie odpowiedzialna za dostarczenie usług dla warstwy dostępowej.

Warstwa dostępowa

Warstwa dostępowa zostanie zbudowana w oparciu o technologię WLAN (wi-fi) zgodnie ze standardem IEEE 802.11 b/g i IEEE 802.11 a/n.

Warstwa dostępowa sieci to newralgiczny element projektowanej infrastruktury, ponieważ odpowiada za obsługę stacji końcowych (Klienckich). Dobór odpowiednich urządzeń w tej warstwie, stanowi bardzo ważny aspekt w procesie projektowania całej infrastruktury, ponieważ sieć dostępowa będzie w całości oparta o urządzenia pracujące w pasmach radiowych, nie wymagających pozwolenia, a w związku z tym, szczególnie podatnych na zakłócenia i interferencje. W Polsce pasma radiowe nie wymagające pozwolenia są uregulowane Rozporządzeniem Ministra Infrastruktury z dnia 24 października 2005r w sprawie urządzeń radiowych nadawczych lub nadawczo- odbiorczych, które mogą być używane bez pozwolenia (Dz.U z 2005r Nr 230, Poz. 1955). Zgodnie z tym rozporządzeniem, urządzenia radiowe mogą być stosowane bez pozwolenia jeżeli spełniają następujące warunki:

a) w paśmie 2400 ÷ 2483,5 MHz - (standard: 802.11b/g)

* stosują modulację szerokopasmową,
* moc wypromieniowywana EIRP jest mniejsza lub różna 100mW

b) w paśmie 5470 ÷ 5725 MHz - (standard 802.11a)

* pozwalają na sterowanie mocą (w zakresie minimum 3dB) w celu uniknięcia zakłóceń,
* umożliwiają dynamiczny wybór częstotliwości (DFS),
* moc wypromieniowywana EIRP jest nie większa niż 1W.

Zadaniem warstwy dostępowej będzie dostarczenie usług dostępu do Internetu dla Beneficjentów końcowych. W tym celu planowana jest instalacja min. 38 tzw. punktów dostępowych, zorganizowanych w ramach 17 tzw. węzłów dostępowych, zlokalizowanych na terenie Gminy Bojanów.

Projekt można będzie uznać za uruchomiony, gdy podczas odbioru systemu komisja powołana przez zamawiającego stwierdzi prawidłowe i wystarczające wykonanie przez system wszystkich założonych funkcji.

1. **SZCZEGÓŁOWE WŁAŚCIWOŚCI I WYMAGANIA FUNKCJONALNO-UŻYTKOWE**
2. **Budowa masztów antenowych oraz konstrukcji wsporczych pod anteny**

Poniższe wymagania ilościowe i konstrukcyjne w zakresie robót i budowlanych należy traktować jako wymagania minimalne. Wykonawca zobowiązany jest do dokonania wizji lokalnej na terenach objętych projektem w celu prawidłowego określenia potrzeb w tym zakresie i prawidłowego skalkulowania kosztów opracowania projektów budowlanych oraz budowy wież i masztów antenowych.

* 1. Budowa masztów antenowych w miejscowościach: Bojanów, Maziarnia, Przyszów i Cisów Las – (min. 4 kpl)

Zaleca się dokonanie wizji lokalnej we wszystkich lokalizacjach, objętych projektem w celu określenia koniczności budowy masztów antenowych oraz ich wysokości.

Zamawiający na prośbę wykonawcy udostępni pełną listę wszystkich jednostek podległych Gminy Bojanów.

Projekt zakłada, budowę masztów antenowych na istniejących obiektach ( budynkach) jednostek podległych Gminy. Dopuszczalne jest również wykorzystanie innych obiektów infrastruktury Gminy Bojanów, po wcześniejszym uzgodnieniu.

Wymagane jest budowa min. 4 szt. masztów antenowych o konstrukcji kratownicowej dla I strefy obciążenia wiatrem. Maszty antenowe, powinny być posadowione na budynkach, stąd ich wysokość powinna być dobrana odpowiednio do warunków i możliwości danego obiektu.

Konstrukcja masztów powinny być złożona z trzonu w postaci kratownicy o przekroju trójkąta równobocznego lub kwadratu z odpowiednią liczbą poziomów odciągów linowych, utrzymujących trzon w stanie równowagi statecznej.

Trzon masztu powinien być podzielony na kilka segmentów co ułatwi jego montaż. Odciągi powinny być zaprojektowane na kierunkach przekątnych, i powinny być wykonane z lin o średnicy minimum ∅10. Na szczycie masztu powinny się znaleźć iglice odgromowe z pręta o średnicy minimum ∅ 16.

Wymagania ogólne

- Wykonawca zobowiązany jest do opracowania wszelkiej niezbędnej dokumentacji, niezbędnej do uzyskania pozwolenia na budowę (jeśli będzie wymagane)

- Przed przystąpieniem do robót budowlanych należy uzyskać wszelkie niezbędne uzgodnienia wynikające z przepisów ustawy „Prawo Budowlane” (Dz.U. nr 89 poz.414).

- maszty powinny być wykonane zgodnie z opracowanym wcześniej projektem budowlanym, oraz z normami i przepisami obowiązującymi w tym zakresie.

- prace montażowe powinny być wykonane przez odpowiednio przeszkolonych pracowników i pod nadzorem osoby posiadającej stosowne uprawnienia budowlane

- prace na wysokości powinny być wykonane przez osoby posiadające aktualne badania lekarskie i przeszkolone do prac wysokościowych.

- 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

* 1. Instalacja wysięgników antenowych oraz konstrukcji wsporczych pod anteny (min. 14 kpl)

Planowana jest instalacja wysięgników antenowych dla pozostałych obiektów jednostek podległych (poza lokalizacjami określonymi wyżej)

Należy zaprojektować i wykonać wysięgniki i uchwyty antenowe o konstrukcji stalowej. Wysokość konstrukcji powinna umożliwiać widoczność optyczną anten na linii beneficjent końcowy - punkt dostępowy. Sposób i miejsce instalacji, należy uzgodnić z administratorami poszczególnych obiektów.

Wymagania ogólne

1. w celu zabezpieczenia urządzeń i kabli w.cz. przed skutkami wyładowań atmosferycznych, konstrukcje wsporcze anten wraz z zamontowanymi na nich antenami oraz ekrany kabli antenowych powinny być uziemione,
2. wszystkie wysięgniki oraz wsporniki antenowe powinny być wykonane zgodnie z normami i przepisami obowiązującymi w tym zakresie,
3. prace powinny być wykonywane pod nadzorem kierownika budowy z uprawnieniami w zakresie konstrukcyjno-budowlanym,
4. prace na wysokości powinny być wykonywane przez osoby posiadające aktualne badania lekarskie i przeszkolenie do prac wysokościowych.

Wymagania gwarancyjne i serwisowe

1. Wykonawca udzieli minimum 36 miesięcznej gwarancji na wykonane konstrukcje.
2. W okresie gwarancji wykonawca zobowiązuje się do usuwania wszelkich wad i nieprawidłowości powstałych na wskutek normalnej eksploatacji.
3. Jeżeli w trakcie okresu gwarancyjnego, istnieje konieczność wykonywania okresowych przeglądów gwarancyjnych, wówczas przeglądy te będą wykonywane na koszt Wykonawcy.
   1. Instalacja szaf teletechnicznych oraz wykonanie instalacji okablowania zasilającego, sygnałowego oraz logicznego pod potrzeby instalacji wyposażenia węzłów dostępowych

We wszystkich lokalizacjach budowy masztów antenowych oraz uchwytów antenowych, 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.)

Lokalizacja szaf dystrybucyjnych oraz sposób prowadzenia instalacji kablowych powinien być wcześniej uzgodniony z właścicielem obiektu.

1. **Budowa sieci szkieletowej (w oparciu o radiolinie cyfrowe) i stacji bazowych WiMAX**.

Szkielet sieci powinien być oparty o cyfrowe radiolinie klasy operatorskiej o minimalnej przepustowości 50 Mb/s FDD, pracujące w szerokim zakresie częstotliwości: 11,13,18,28,32,38 GHz (poprzez dobór odpowiedniego ODU).

Szkielet sieci powinien być oparty o minimum 4 Węzły Rdzeniowe sieci, proponowane lokalizacje:

* WR1 – w miejscowości Bojanów
* WR2 – w miejscowości Maziarnia
* WR3 – w miejscowości Przyszów
* WR4 – w miejscowości Cisów Las

Węzeł Rdzeniowy WR1 w miejscowości Bojanów, powinien zostać wyposażony dodatkowo w stację bazową WiMAX.

Wyposażenie Stacji Bazowej należy dobrać w taki sposób aby możliwe było podłączenie do sieci jednostek podległych Gminy Bojanów, objętych projektem.

Niniejszy dokument zawiera specyfikację minimalnych wymagań w tym zakresie.

* 1. Radiolinie cyfrowe 50 Mb/s FDD (min. 4 kpl.)  
     **Cecha A**

Wymagania ogólne

- Wykonawca jest zobowiązany do opracowania dokumentacji projektowej w zakresie budowy sieci szerokopasmowej, której elementem będzie planowanie radiowe, a co za tym idzie odpowiedni dobór częstotliwości oraz parametrów pracy radiolinii tak aby osiągnąć dostępność pracy 99.995 % średniorocznie.

- Wykonawca zobowiązany jest do przygotowania stosownej dokumentacji do Urzędu Komunikacji Elektronicznej w celu uzyskania pozwolenia radiowego przez Zamawiającego

Wymagania techniczne:

* Część wewnętrzna radiolinii (IDU) powinna mieć możliwość współpracy z systemem zewnętrznych jednostek radiowych (ODU) mogących pracować w następujących pasmach: 13, 18, 23, 28, 32, 38 GHz
* Radiolinia powinna umożliwiać transmisję w kanałach radiowych o następującej szerokości: 7/14/28/56 MHz
* Dla każdej szerokości kanału radiowego dostępne muszą być następujące modulacje: QPSK, 16QAM, 32QAM, 64QAM, 128QAM oraz 256 QAM
* Automatyczna regulacja Mocy nadajnika (ATPC): wymagany zakres ATPC : min. 20 dB
* Radiolinia powinna być dostarczona w konfiguracji 1+0 i mieć możliwość rozbudowy do konfiguracji 1+1 Hot Standby (pełna redundancja).
* Architektura (IDU i ODU rozdzielne kablem IF)
* Połączenie IDU –ODU – za pomocą kabla koncentrycznego typu RG-8, LDF-1, LCF-1 lub równoważnego
* Radiolinia musi być wyposażona w wentylator chłodzący jednostkę wewnętrzną IDU
* Zasilanie: napięcie standardowe -48 VDC

Wymagane możliwości rozbudowy (bez zmiany lub dodania jakiejkolwiek części sprzętowej, jedynie poprzez zmianę klucza licencyjnego – programowo):

* Obsługa modulacji adaptacyjnej w pełnym zakresie pracy: od QPSK do 256QAM.
* Wymagane jest bezstratne przełączanie modulacji w trybie adaptacyjnym (brak jakichkolwiek błędów transmisyjnych (ES, SES, BBE) lub opóźnień przy przełączaniu)
* Rozbudowa przepustowości systemu do trybu 256QAM w kanale 56MHz
* Wymagania dotyczące interfejsów i protokołów transmisyjnych

Wymaga się aby była wyposażona w następujące interfejsy zewnętrzne (możliwe do przeznaczenia na transmisję ruchu) w minimalnej liczbie:

* 1x 10/100/1000Base-T – elektryczny
* 1 x gniazdo SFP z możliwością dołączenia optyki niezależnego producenta
* 5 x 10/100Base-T
* 16x E1 - 120 Ohm
* Licencja producenta radiolinii w chwili jej dostawy powinna umożliwiać transmisję ruchu z wykorzystaniem przynajmniej jednego portu 10/100/1000Base-T.
* Radiolinia musi wspierać następujące standardy Ethernet/IP:  
  802.3, 802.3u, 802.3ab, 802.3z, 802.3ac, 802.1Q, 802.1p, 802.1ad, 802.3x, 802.3ad, 802.1D, 802.1w, 802.1s, RFC 1349, RFC 2474, RFC 2460

Wymagane możliwości rozbudowy (jedynie poprzez zmianę licencji):

* Wymagane jest posiadanie Certyfikatów Metro Ethernet Forum --- przynajmniej MEF-9 & MEF-14 dla usług (EPL, EVPL & E-LAN)
* Radiolinia musi być fizycznie gotowa do pracy jako switch Metro Ethernetowy obsługujący:
* Min. 4000 aktywnych VLANów
* Min. 8000 MAC adresów
* Min. 5 portów 100-Base-T
* 1x 10/100/1000Base-T
* 1x gniazdo SFP z możliwością obsadzenia wkładką optyczną niezależnego producenta
* Radiolinia musi mieć możliwość nadania dla kanałów E1 priorytetu różnicującego kolejność wyłączania interfejsów T1/E1 w przypadku degradacji jakości łącza radiowego i dynamicznej zmiany modulacji na niższą – przynajmniej dwa priorytety

Zarządzanie:

* Radiolinia mus być wyposażona w możliwość zarządzania lokalnego:
* poprzez interfejs Ethernet (przynajmniej dwa)
* poprzez interfejs RS-232
* Zarządzanie zdalne:

Bezpieczne zarządzanie za pomocą:

* dedykowanego systemu zarządzania – pracującego na platformie Microsoft Windows
* poprzez HTTP oraz HTTPS
* poprzez Telnet oraz SSH (z możliwością wyłączenia Telnet)
* dowolnej aplikacji SNMP – wymagane dostarczenie pliku MIB
* Trap Serwer:
* Możliwość konfiguracji minimum czterech różnych adresów serwerów do zapisu logów i alarmów (Trap Server),

Kompatybilność ze standardami:  
ITU-T G.703, G.736, G.775, G.823, G.824, G.828, ITU-T I.432, ETSI ETS 300 147, ETS 300 417

Wymagania ogólne względem system zarządzania

Do zamawianych radiolinii powinien być dołączony system zarządzania wspierający przynajmniej następujące funkcjonalności:

* Zbiorcze zarządzanie wieloma linkami radiowymi - minimum dwudziestoma elementami sieci (np. połówkami radiolinii) w chwili dostarczenia z możliwością skalowalnej rozbudowy
* Zarządzanie alarmami (zbieranie, potwierdzanie przez operatora)
* Zarządzanie jakością sieci (pobieranie i przechowywanie statystykami Performance pobieranymi z zarządzanych elementów sieci)
* Zarządzanie bezpieczeństwem (przynajmniej dwa poziomy uprawnień użytkowników systemu)
* Upgrade software (zbiorcze zarządzanie uaktualnieniami oprogramowania sprzętowego radiolinii)
* Logowanie zdarzeń,
* Wizualizacja sieci (graficzne przedstawienie rozlokowania elementów systemu np. w postaci mapy)
* Backup konfiguracji zarządzanych elementów (możliwość tworzenia kopii zapasowych konfiguracji zarządzanych radiolinii)
* Automatyczne dodawanie elementów (możliwość automatycznego dodawania nowych elementów do systemu po podaniu warunków początkowych np. podsieć IP do skanowania)
* Masowa zmiana konfiguracji wszystkich elementów – przynajmniej masowa zmiana czasu, bądź adresu serwera NTP, lub trap serwera SNMP

Warunki środowiskowe.

Urządzenia sieci radioliniowej musza spełniać następujące wymagania środowiskowe :

* dla modułów zainstalowanych wewnątrz pomieszczeń praca bez pogorszenia parametrów w temperaturze od +5o do +45oC przy wilgotności 30%, oraz

od +5o do + 300C przy wilgotności 95%

* dla modułów zainstalowanych na zewnątrz pomieszczeń praca bez pogorszenia parametrów w temperaturze od -25o do +55oC przy wilgotności 30%,

oraz od -30o do +30oC przy wilgotności 100%; odporność na wiatr : przetrwanie nie mniej niż 200 km/h

Wymagania gwarancyjne i serwisowe

- W celu zachowania pełnej kompatybilności i spójności rozwiązania, oraz uproszczenia zarządzania i administracji – wszystkie radiolinie powinny być fabrycznie nowe i pochodzić od jednego producenta

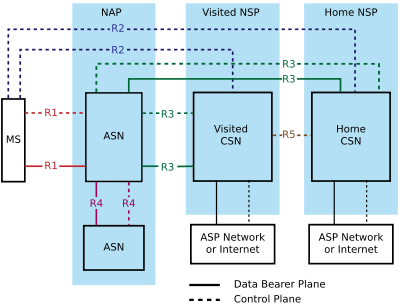
- Urządzenia powinny być objęte minimum 36 miesięczną gwarancją producenta.

- W okresie gwarancji (36 miesiące) Wykonawca powinien zapewnić gotowość serwisową polegająca na naprawie lub podmianie sprzętu w razie awarii, najpóźniej następnego dnia roboczego, od momentu zgłoszenia usterki.

* 1. Stacja Bazowa WiMAX – (min. 2 kpl.)

**Cecha B**

* System powinien być w pełni zgodny ze standardem 802.16e-2005 i pracować w paśmie częstotliwości 3.6-3.8GHz.
* System powinien posiadać architekturę zgodną ze standardem 802.16e-2005 tak jak to określono w sieciowym modelu odniesienia (*ang.: Network Reference Model – NRM*) poniżej.

[](http://en.wikipedia.org/wiki/File:WiMAXArchitecture.svg)

* Elementy systemu zdefiniowane przez blok funkcjonalny ASN (*ang.: Access Service Network*) powinny być skonstruowane w sposób umożliwiający poprawną pracę według profili A, B lub C, zgodnie z architekturą sieci określoną przez organizację WiMAX Forum
* Stacja bazowa systemu powinna posiadać kompaktową obudowę przystosowaną do instalacji zewnętrznych (t.zw. rozwiązanie „All Outdoor” gdzie brak jest urządzeń aktywnych instalowanych wewnątrz pomieszczeń) zawierającą w pojedynczej obudowie kompletną część radiową, modemową, procesor/kontroler, ASN-GW oraz antenę sektorową. Stacja bazowa powinna posiadać również odpowiednie złączna do podłączenia, zewnętrznego ASN-GW oraz systemu GPS.
* System powinien pracować poprawnie zarówno przy zachowaniu widoczności optycznej pomiędzy stacją bazową a terminalem abonenckim (*ang.: LOS*) jak również bez takiej widoczności (*ang.: NLOS*) lub ograniczonej (*ang.: nLOS*).
* System powinien poprawnie obsługiwać w tym samym czasie co najmniej takie usługi jak głos, wideo, dostęp do internetu
* System powinien obsługiwać użytkowników mobilnych (tak jak definiuje to standard 802.16e), nomadycznych oraz zapewniać łącza stałe.
* System powinien obsługiwać technologię SOFDMA.
* System powinien obsługiwać kanały radiowe od 5MHz z 512 punktami FFT do 10MHz z 1024 punktami FFT bez konieczności wymiany sprzętu lub dokonywania uaktualnienia oprogramowania.
* System powinien obsługiwać technikę “Forward Error Correction” (FEC).
* System powinien obsługiwać technikę „Turbo Coding” 1/2, 2/3, 3/4 oraz 5/6.
* System powinien obsługiwać modulacje QPSK, QAM16, QAM64 z wykorzystaniem techniki korekcji błędów „Cyclic Turbo Code” zapewniając modulację QAM64 5/6 zarówno dla kierunku transmisji w stronę sieci (*ang: downlink*) jak i w stronę abonenta (*ang.: uplink*).
* System powinien obsługiwać zaawansowane techniki antenowe MIMO Tx drugiego rzędu (2 Tx) pracujące zarówno w trybie MIMO A jak również MIMO B z funkcją automatycznego przełączania pomiędzy trybami
* System powinien obsługiwać technologię “Rx diversity” (MRRC) drugiego rzędu (2 Rx) dla kierunku transmisji w stronę abonenta (*ang.: uplink*)
* System powinien zapewniać zwiększoną odporność na zakłócenia poprzez wielokrotne rozgłaszanie opisu dostępu w pojedynczej ramce (MAP).
* System powinien obsługiwać technikę HARQ.
* System powinien posiadać wbudowany analizator widma
* System powinien obsługiwać technikę automatycznej kontroli mocy transmisyjnej (*ang.: Automatic transmit power control - ATPC*).
* Zmiany modulacji w systemie (QPSK, QAM16, QAM64) powinny następować automatycznie w sposób dynamiczny.
* System powinien pracować w technologii TDD (*ang.: Time Division Duplex*) wykorzystując co najmniej następujące szerokości kanałów: 5MHz, 7MHz, 10MHz, 2x7MHz oraz 2x10MHz
* Moc transmisyjna nadajnika radiowego mierzona na porcie RF anteny nie może być mniejsza niż 30 dBm.
* System powinien być zasilany ze źródła napięcia stałego -48Vdc.
* System powinien obsługiwać jednocześnie technikę ETH-CS oraz IP-CS
* System powinien posiadać wbudowany serwer DHCP i obsługiwać opcję 82 oraz DHCP opcja trybu transparentnego
* System powinien obsługiwać mechanizmy klasyfikacji ruchu w oparciu o DSCP, PPPoE, VLAN priority lub VLAN ID
* System powinien obsługiwać mechanizm 802.1Q tagging.
* System powinien posiadać elastyczną architekturę umożliwiającą lokalne lub centralne (przez serwer AAA) kreowanie usług jednocześnie pracując w trybie centralnego lub rozproszonego (wbudowanego w systemie) ASN-GW.
* Mechanizm autentykacji w systemie powinien odbywać się za pomocą protokołu RADIUS poprzez EAP-TTLS
* System powinien obsługiwać algorytmy kodowania AES 128bit. Klucze AES powinny być generowane w sposób dynamiczny przy każdorazowym logowaniu się użytkownika w sieci.
* System powinien posiadać mechanizmy “uczenia się” adresów MAC w celu zapewnienia optymalizacji ruchu (zapobieganie przepełnieniu).
* Stacja bazowa systemu powinna być wyposażona w interfejs Ethernet 100/10 MB/s w celu podłączenia stacji do sieci transmisyjnej (szkieletowej).
* System powinien umożliwiać wykorzystanie tylko jednego odbiornika GPS do synchronizacji co najmniej 4 stacji bazowych zainstalowanych w jednej lokalizacji.
* Stacja Bazowa powinna mieć możliwość zasilania elektrycznego zgodnego ze standardem PoE (*ang.: Power over Ethernet*), Jednostki Abonenckiej służącej jako dostęp do sieci szkieletowej za pomocą wbudowanego w Stację Bazową interfejsu sieciowego.
* Obudowa systemu powinna posiadać Współczynnik Ochrony IP65

Wymagania gwarancyjne i serwisowe

* Wymagany jest 36 miesięczny serwis  gwarancyjny na wszystkie urządzenia WiMax,  (Cechy: B, C, E) świadczony w następującym zakresie:

- przyjmowanie zgłoszeń bezpośrednio w godzinach od 8:00-16:00 w dni robocze

- naprawa lub wymiana w następny dzień roboczy od pisemnego zgłoszenia lub mailem)

- prawo do aktualizacji oprogramowania systemowego

* 1. System zarządzania WiMAX (1 szt.)

**Cecha C**

Wymagania funkcjonalne

* Automatyczne i manualne wykrywanie elementów sieci takich jak Stacje Bazowe, Jednostki Abonenckie itp. System powinien zachowywać dane wszystkich elementów systemu.
* Zarządzanie Jednostkami Abonenckimi powinno odbywać sie za pomocą protokołu TR-69.
* System powinien zapewniać łatwość obsługi, intuicyjny interfejs webowy oraz wszechstronny podręcznik użytkownika/pomoc systemu.
* Filtry i wyszukiwanie: powinno być możliwe predefiniowanie filtrów użytkownika pozwalających na przeszukiwanie takich danych jak: alarmy oraz elementy sieci.
* Bezpieczeństwo: zaimplementowane mechanizmy kontroli i ograniczania dostępu do system zarządzania
* Możliwość zdalnego wgrania oprogramowania przez radio.
* Wszechstronne zarządzanie za pomocą protokołu SNMP.
* Administracja Systemem
* Dodawanie/zmiana/konfiguracja/weryfikacja/usuwanie/zarządzanie kontem użytkownika końcowego w systemie
* Dodawanie/zmiana/konfiguracja/weryfikacja/usuwanie/zarządzanie elementów sieci w bazie danych.
* Dodawanie/zmiana/konfiguracja/weryfikacja/usuwanie/zarządzanie lokalizacjami w systemie.
* Powinna być możliwa kontrola i ograniczanie praw, przywilejów oraz autoryzacji operatora.
* Kontrola dostępu powinna umożliwiać klasyfikację grup operatorów ze wspólnymi charakterystycznymi prawami, z możliwością ograniczenia lub rozszerzenia praw dostępu dla pojedynczego użytkownika.
* Możliwość ograniczenia dostępu do elementów sieci oraz/lub do logów.
* Powinny być dostępne logi wszystkich wiadomości pomiędzy Systemem Zarządzania I Elementami Sieci.
* Powinna być możliwość oceny Operatora, który zainicjował wiadomość.
* Powinna być możliwość definiowania Użytkowników z różnymi wymaganiami dot. klas usługowych. Powinna być możliwość wpierania klas usługowych dla takich aplikacji jak głos czy multimedia.
* Zarządzanie urządzeniami.
* Automatyczne i manualne wykrywanie elementów sieci takich jak Stacje Bazowe, Jednostki Abonenckie itp. System powinien zachowywać dane wszystkich elementów systemu.
* Pokazywanie podłączonych elementów sieci korzystając z bazy danych, dając kompletny widok sieci bez fizycznego sprawdzania każdego ze zdalnych urządzeń
* Zarządzanie alarmami: Alarmy powinny być zbierane z całej sieci, przechowywane w bazie danych i pokazywane zgodnie z użytym filtrem w widoku alarmów.
* Zarządzanie kontrolą jakości pracy elementów sieci.
  1. Przełączniki dystrybucyjne 24 porty 10/100, (min. 4 szt.)

**Cecha D**

Wymagania ogólne

* W celu zachowania pełnej kompatybilności i spójności rozwiązania, oraz uproszczenia zarządzania i administracji - wszystkie urządzenia aktywne sieci (Cechy: D, G, I, L, M, N, O) powinny pochodzić 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 oparte na oficjalnej gwarancji świadczonej przez producenta sprzętu.
* Zamawiający oczekuje, że sprzęt dostarczony w ramach realizacji umowy będzie sprzętem zakupionym w oficjalnym kanale sprzedaży producenta. Co zgodnie z opisem wyżej, będzie on sprzętem nowym i posiadającym stosowny pakiet usług gwarancyjnych kierowanych również do użytkowników z obszaru Rzeczpospolitej Polskiej.

Wymagania techniczne

* urządzenie o stałej konfiguracji
* min. 64MB pamięci DRAM oraz 32MB pamięci Flash
* obsługa min. 8000 adresów MAC
* wydajność przełączania co najmniej 16 Gbps oraz przepustowość co najmniej 6,5 Mpps dla pakietów 64 bajtowych;
* co najmniej 24 porty FastEthernet w standardzie 10/100BaseTX w tym 8 z funkcjonalnością PoE (IEEE 802.3af ) oraz dwa porty typu combo mogące pracować jako 10/100/1000BASE-T oraz 1000BaseX ze stykiem definiowanym przez SFP, GBIC lub równoważne.
* automatyczne wykrywanie przeplotu (AutoMDIX) na portach miedzianych
* wbudowane narzędzia do diagnozy okablowania na portach miedzianych (time domain reflector)
* obsługa co najmniej 255 sieci VLAN i 4000 VLAN ID
* obsługa mechanizmów dystrybucji informacji o sieciach VLAN pomiędzy przełącznikami
* obsługa protokołów sieciowych zgodnie ze standardami:

- IEEE 802.1x

- IEEE 802.1s

- IEEE 802.1w

- IEEE 802.3x full duplex dla 10BASE-T i 100BASE-TX

- IEEE 802.3ad

- IEEE 802.1D

- IEEE 802.1p

- IEEE 802.1Q

- IEEE 802.3 10BASE-T

- IEEE 802.3u 100BASE-TX

- IEEE 802.3z 1000BASE-X

- IEEE 802.3ab 100BASE-T

* mechanizmy związane z zapewnieniem jakości usług w sieci:

- obsługa co najmniej czterech kolejek sprzętowych, wyjściowych dla różnego rodzaju ruchu

- mechanizm automatycznej konfiguracji portów do obsługi VoIP

- możliwość ograniczania pasma dostępnego na port (rate limiting) z granulacją co 1Mbps dla ruchu wejściowego i wyjściowego

* mechanizmy związane z zapewnieniem bezpieczeństwa sieci:

- dostęp do urządzenia przez konsolę szeregową, SSHv2 i SNMPv3

- możliwość autoryzacji prób logowania do urządzenia za pomocą serwerów RADIUS lub TACACS+

- możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. protected ports) z pozostawieniem możliwości komunikacji z portem nadrzednym (designated port) lub funkcjonalność private VLAN (w ramach portu)

- monitorowanie zapytań i odpowiedzi DHCP (tzw. DHCP Snooping)

- możliwość tworzenia portów monitorujących, pozwalających na kopiowanie na port monitorujący ruchu z innego dowolnie wskazanego portu lub sieci VLAN z lokalnego przełącznika

- ochrona przed rekonfiguracją struktury topologii Spanning Tree spowodowana przez niepowołane i nieautoryzowane urządzenie sieciowe

- obsługa list kontroli dostępu (ACL) z uwzględnieniem adresów MAC i IP, portów TCP/UDP bez spadku wydajności urządzenia

- min. 5 poziomów uprawnień do zarządzania urządzeniem (z możliwością konfiguracji zakresu dostępnych funkcjonalności i komend)

- współpraca z systemami kontroli dostępu do sieci typu NAC, NAP itp.

* obsługa ruchu multicast z wykorzystaniem IGMPv3
* obsługa grupowania portów w jeden kanał logiczny zgodnie z LACP
* możliwość uruchomienia funkcji serwera DHCP
* plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nie ulotnej powinno być możliwe uruchomienie urządzenia z nowa konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian możliwość zarządzania przy pomocy bezpłatnej aplikacji graficznej dostarczanej przez producenta
* możliwość łączenia przełączników we wspólnie zarządzanie klastry
* możliwość zastosowania zewnętrznego redundantnego zasilacza
* możliwość montażu w szafie 19”
* obudowa wykonana z metalu

Wymagania gwarancyjno serwisowe

* Wymagany jest 36 miesięczny serwis  gwarancyjny na wszystkie urządzenia aktywne,  (Cechy: D, G, I, L, M, N, O) świadczony bezpośrednio przez producenta urządzeń w następującym zakresie:

- przyjmowanie zgłoszeń bezpośrednio przez producenta w godzinach od 8:00-16:00 w dni robocze

- naprawa lub wymiana w następny dzień roboczy od pisemnego zgłoszenia awarii (faxem lub mailem)

- bezpośredni dostęp do wsparcia technicznego producenta sprzętu

- prawo do aktualizacji oprogramowania systemowego

* Serwis gwarancyjny musi być oparty na świadczeniach gwarancyjnych producenta.
* Zaproponowany pakiet serwisowy musi zapewniać bezpośrednie zgłoszenie awarii sprzętu do producenta sprzętu (a nie tylko u Wykonawcy) przez cały okres trwania gwarancji.

1. **Budowa warstwy dystrybucyjnej i dostępowej sieci (14 Węzłów Dystrybucyjnych i min . 38 Punktów Dostępowych)**

Planowana jest budowa min 14 Węzłów Dystrybucyjnych. Minimalne wymagane wyposażenie Węzłów Dystrybucyjnych powinno zawierać:



- terminal CPE WiMAX (dotyczy min. 9 lokalizacji WD, Jednostek Podległych objętych projektem)

- punkt dostępowy WLAN (802.11a/g/n) MIMO

- anteny sektorowe 2,4 GHz i 5GHz MIMO

- zarządzalny przełącznik dostępowy z portami PoE

- infrastruktura dodatkowa (uchwyty i wysięgniki antenowe, szafki 19’’, okablowanie zasilające i sygnałowe, inne)

**Uwaga!**

Zaleca się dokonanie wizji lokalnej we wszystkich lokalizacjach, w których planowana jest instalacja Węzłów Dystrybucyjnych (spis wszystkich lokalizacji zawiera tabela poniżej) w celu prawidłowego wyliczenia kosztów związanych z ich budową.

Lokalizacja szaf dystrybucyjnych, sposób prowadzenia instalacji zasilającej i sygnałowej powinien być wcześniej uzgodniony z właścicielem obiektu.

Tabela poniżej zawiera wykaz lokalizacji Węzłów Dystrybucyjnych

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **OZNACZENIE WĘZŁA** | **LOKALIZACJA** | |
| **Nazwa** | **Współrzędne/adres** |
| 1 | WD1 | Bojanów, Gminny Ośrodek Kultury | N 50o 25' 19,70”  E 21o 56' 43,36” |
| 2 | WD2 | Bojanów, Szkoła Podstawowa nr 1 | N 50o 25' 19,70”  E 21o 56' 43,36” |
| 3 | WD3 | Bojanów, Gimnazjum nr1 | N 50o 25' 19,70”  E 21o 56' 43,36” |
| 4 | WD4 | Bojanów, Szkoła Podstawowa nr 2 | N 50o 24' 43,99”  E 21o 56' 52,33” |
| 5 | WD5 | Bojanów, Gminna Biblioteka Publiczna | Ul. Strażacka 1  37-433 Bojanów |
| 6 | WD6 | Stany, Dom Kultury, biblioteka | N 50o 26’ 22,58”  E 21o 58' 45,5” |
| 7 | WD7 | Stany, Szkoła Podstawowa nr 2 | N 50o 26' 10,17”  E 21o 58' 47,13” |
| 8 | WD8 | Stany, Gimnazjum nr2 | N 50o 26' 10,17”  E 21o 58' 47,13” |
| 9 | WD9 | Przyszów, Dom Kultury | N 50o 28' 57,14”  E 21o 59' 43,29” |
| 10 | WD10 | Przyszów, Szkoła Podstawowa, Przedszkole | N 50o 28' 50,95”  E 21o 59' 44,80” |
| 11 | WD11 | Maziarnia, Dom Kultury | N 50o 27' 28,65”  E 22o 01' 20,06” |
| 12 | WD12 | Maziarnia, Szkoła Podstawowa | N 50o 27' 19,22”  E 22o 01' 51,05” |
| 13 | WD13 | Gwoździec, Szkoła Podstawowa | N 50o 22' 18,04”  E 22o 00' 03,92” |
| 14 | WD14 | Gwoździec, Dom Kultury | N 50o 22' 34,89”  E 21o 59' 24,15” |
| 15 | WD 15 | Korabina, budynek byłej szkoły  Świetlica wiejska | Korabina 25,  Korabina nr ewid. dz. 441 |
| 16 | WD 16 | Przyszów Ruda, świetlica wiejska | Ruda 38 |
| 17 | WD 17 | Laski , świetlica wiejska Remiza OSP | Laski 33,  Laski 38 |
| 18 | WD 18 | Cisów Las, świetlica wiejska | Cisów Las 31 |
| 19 | WD 19 | Stany, Remiza OSP | Stany ul. Strażacka 1 |
| 20 | WD 20 | Stany, budynek oczyszczalnia ścieków | Stany, nr ewid. działki 5335/1 |

* 1. Terminal radiowy WiMAX - zewnętrzny (min. 10 szt.)

**Cecha E**

Wymagania techniczne

* Terminal abonencki powinien być w pełni zgodny ze standardem 802.16e-2005
* Terminal abonencki powinien zapewnić prawidłowe działanie ze stacją bazową systemu na podstawie testów certyfikacyjnych 802.16e-2005 wave 2 określonych przez organizację WiMAX Forum
* Terminal abonencki powinien pracować w paśmie częstotliwości 3.6-3.8GHz oraz zapewnić prawidłowe działanie ze stacją bazową systemu oraz przy zastosowaniu testów certyfikacyjnych 802.16e-2005 wave 2 określonych przez organizację WiMAX Forum
* Terminal abonencki powinien obsługiwać skalowalną technologię OFDMA 512/1024 FFT (ang.: scalable OFDMA)
* Terminal abonencki powinien pracować w technologii TDD (ang.: Time Division Duplex)
* Terminal abonencki powinien obsługiwać modulacje QPSK, QAM16 oraz QAM64.
* Terminal abonencki powinien obsługiwać zaawansowane techniki antenowe MIMO pracujące zarówno w trybie MIMO A jak również MIMO B oraz technikę MRC (ang.: Maximum Ratio Combining)
* Terminal abonencki powinien posiadać dwie opcje konfiguracyjne: opcja z anteną zintegrowaną (część zewnętrzna radiowa jest zintegrowana z anteną w sposób kompaktowy) oraz opcja z anteną oddzielną (wymagany jest interfejs RF w części radiowej do podłączenia odrębnej anteny)
* Maksymalna moc transmisyjna terminala abonenckiego mierzona na porcie radiowym RF anteny nie powinna być niższa niż 21 dBm.
* Terminal abonencki powinien zapewniać możliwość klasyfikacji ruchu oraz funkcje zapewniania jakości usług (ang.: Quality of Service – QoS) w oparciu o mechanizm IP DSCP (ang.: Differentiated Services Code Point)
* Terminal abonencki powinien obsługiwać funkcjonalność IP CS (w trybie „bridge”) z transparentnym ruchem DHCP
* Terminal abonencki powinien obsługiwać funkcjonalność ETH CS z możliwością klasyfikacji ruchu DSCP, PPPoE, VLAN ID (802.1q), VLAN priority (802.1p)
* Jednostka Abonencka powinna wykorzystywać funkcjonalność multi-host czyli możliwość pracy z co najmniej dwoma adresami IP na porcie WAN.
* Terminal abonencki powinien być zarządzany lokalnie lub zdalnie za pomocą zwykłej przeglądarki internetowej
* Jednostka abonencka powinna obsługiwać protokół TR-069 lub OMA-DM dla centralnego zarządzania za pomocą oprogramowania ACS
* Terminal abonencki powinien obsługiwać algorytmy kodowania AES 128bit
* Temperatury otoczenia w jakich terminal abonencki powinien działać poprawnie powinny wynosić co najmniej: od -5C do 45C dla części wewnętrznych terminala oraz od -40C do 55C dla części zewnętrznych
* Terminal abonencki powinien być wyposażony w interfejs Ethernet (RJ-45) z funkcją PoE (ang.: Power over Ethernet)

Wymagania gwarancyjne i serwisowe

- zgodnie z wymaganiami określonymi w rozdziale V podpunkt 2.2

* 1. Połączenia dystrybucyjne punkt-punkt - (min. 10 kpl.)

**Cecha F**

Wymagania techniczne

* Urządzenie przeznaczone do zastosowań zewnętrznych typu punkt-punkt (wyposażone w zestaw montażowy),
* Temperatura pracy: od -30C do 80C,
* Wilgotność pracy: 5 to 95%,
* Procesor: Atheros MIPS 24KC, 400MHz,
* Pamięć: 64MB SDRAM, 8MB Flash,
* Wyposażone w interfejs sieciowy 10/100 BASE-TX (Cat. 5, RJ-45),
* Pobór mocy:max. 8 Watt,
* Zasilanie: 24V POE Adapter (POE-24),
* Metoda zasilania: Pasywny POE,
* Waga: max. 3.82 kg,
* Rozmiar: max. 445 x 416 x 34mm
* Regulacje prawne: Potwierdzenia FCC Part 15.247, IC RS210, CE, RoHS, ETSI 300-019-1.4,
* Urządzenie zintegrowane z dwu-polaryzacyjną anteną o zysku minimum 24,8dBi
  + Częstotliwość pracy: 4.9GHz-6.0GHz
  + 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. 150 Mbps dla ruchu TCP/IP,
* Pracuje w trybach: router lub bridge,
* InterfejsWiFiwspieratryby Access Point, Access Point WDS, Client, Client WDS.
* System do centralnego zarządzania min. 100 urządzeniami

Wymagania gwarancyjne i serwisowe

- Urządzenia powinny być objęte minimum 36-miesięczną gwarancją producenta.

* 1. Przełączniki dostępowe 8 port 10/100 8xPoE – (min. 20 szt.)

**Cecha G**

Wymagania techniczne

* 8 portów RJ-45 10/100,
* 2 porty RJ-45 10/100/1000,
* 2 gniazda mini-GBIC (współdzielone z portami GE),
* port konsoli,
* autonegocjacja dupleksu i prędkości,
* samokrosujące się porty (Auto-MDI/MDIX),
* obsługa VLAN 802.11q (do 256 grup),
* tryby przyporządkowania portu do VLANu:
  + statyczny,
  + dynamiczny,
* obsługa ramek jumbo do 1632 bajtów,
* tablica adresów MAC 8kB,
* przepustowość wewnętrzna **5.6Gbps** non blocking,
* QoS - przyporządkowywanie wag WRR (Weight Round Robin) / CoS (Class of *Service*) dla 4 kolejek na każdym porcie przełącznika:
  + Port-based,
  + 802.1p VLAN priority based,
  + IP TOS/DSCP based,
  + IPv4 Traffic Class based COS,
  + IPv6 Traffic Class based COS,
  + TCP/UDP Port based,
  + Diffserv,
  + Classification and Remarking ACLs,
  + Limitowanie pasma: ruch przychodzący / ruch wychodzący,
* port mirroring - przekierowywanie ruchu z fizycznego portu na inny port,
* konfiguracja z poziomu przeglądarki WWW (http / https), SNMP v.1, 2c, 3, RMON,
* możliwość aktualizaji firmware'u (TFTP, przeglądarka internetowa HTTP),
* inne opcje zarządzania - Telnet (Menu-driven configuration):
  + Secure Shell (SSH),
  + RADIUS,
  + TACACS,
  + Telnet Client,
  + Secure Socket Layer (SSL),
  + Switch Audit Log,
  + DHCP Client,
  + BootP,
  + SNTP,
  + Xmodem upgrade,
  + Syslog,
* bezpieczeństwo: uwierzytelnianie użytkowników za pomocą protokołu 802.1x - Radius Authentication, MD5 Encryption, kontrola dostępu:
  + Source and Destination MAC-based,
  + Source and Destination IP address,
  + Protocol,
  + TOS/DSCP,
  + Port,
  + VLAN,
  + Ethertype,
* agregacja portów: do 8 portów w 8 grupach, obsługa LCAP (802.3ad),
* storm control: możliwość ograniczenia rozsyłania ramek broadcast / multicast / unknown unicast,
* spanning tree - IEEE 802.1d Spanning Tree, IEEE 802.1s Multiple Spanning Tree, IEEE 802.1w Rapid Spanning Tree, Fast Linkover,
* IGMP Snooping - IGMP (v1/v2) wsparcie do 256 grup multicast,
* testy okablowania miedzianego z poziomu przełącznika, ping, traceroute,
* diody: System, Link/Act, PoE,
* zasilacz zewnętrzny,
* technologia Power over Ethernet (7.5W na 8 portach i 15.4W na 4 portach),
* chłodzenie: aktywne,
* temperatura pracy: 0 - 40 stopni C,
* temperatura przechowywania: -20 - 70 stopni C,
* wilgotność środowiska pracy: 10% - 90%,
* wilgotność środowiska przechowywania: 10% - 95%,
* wymiary: 279.4 x 44.5 x 170mm,
* waga: 1,2kg,

Wymagania gwarancyjne i serwisowe

- Urządzenia powinny być objęte minimum 36-miesięczną gwarancją producenta.

* 1. UPS 1000VA RACK (min. 20 szt.)

**Cecha H**

Wymagania techniczne

* Moc pozorna 1000VA
* Moc rzeczywista 600 Wat
* 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 producenta

* 1. Bezprzewodowy punkt dostępu 802.11a/g/n 2x2 MIMO (min. 38 szt.)

**Cecha I**

Wymagania techniczne

* Urządzenia powinny współpracować z kontrolerem sieci bezprzewodowej WLAN i powinny z nim tworzyć spójny i jednorodny system.
* Urządzenie powinno posiadać pamięć typu Flash nie mniejsza niż 16MB.
* Urządzenie powinno posiadać pamięć typu DRAM nie mniejsza niż 32MB.
* Powinno posiadać port 10/100/1000BASE-T
* Powinno posiadać port do lokalnego zarządzania w trybie tekstowym
* Powinno mieć możliwość obsługi co najmniej 16 sieci wirtualnych (VLAN).
* Powinno posiadać złącza antenowe:
  + 802.11a: 3 złącza RP-TNC,
  + 802.11b/g/n: 3 złącza RP-TNC.
* Posiadać 2 osobne moduły radiowe dla częstotliwości 2,4Ghz oraz 5Ghz:
  + Czułość modułu 2.4Ghz: -101dBm
  + Czułość modułu 5Ghz: - 93dBm
* Zgodność ze standardami IEEE:
  + IEEE 802.11a/b/g,
  + IEEE 802.11n 2.0,
    - 2x3 multiple-inputmultiple-output (MIMO) z dwoma strumieniami przestrzennymi
    - Maximal ratio combining (MRC)
    - Formowaniefali
    - szerokośćkanałów 20- i 40-MHz
    - PHY przepływności do 300 Mbps
    - Agregacja pakietów: A-MPDU (Tx/Rx), A-MSDU (Tx/Rx)
    - 802.11 Dynamicznywybórkanału (DFS)
    - Wsparcie: Cyclic shift diversity (CSD)
  + IEEE 802.11h,
  + IEEE 802.11d
* Mechanizmy bezpieczeństwa:
  + 802.11i, Wi-Fi Protected Access 2 (WPA2), WPA
  + 802.1X
  + Advanced Encryption Standards (AES), Temporal Key Integrity Protocol (TKIP)
  + Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
  + EAP-Tunneled TLS (TTLS) or Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2)
  + Protected EAP (PEAP) v0 or EAP-MSCHAPv2
  + Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)
  + PEAPv1 or EAP-Generic Token Card (GTC)
  + EAP-Subscriber Identity Module (SIM)
* Wsparcie dla Multimediów:
  + Wi-Fi Multimedia (WMM™) – rozszerzenie 802.11e
* Wspierać zasilanie przez:
  + Siec Ethernet zgodnie ze standardemIEEE 802.3af PoE
  + Lokalny zasilacz
* Pobór mocy: max. 15.4 Watt,
* Wymiary: max. 22.1 x 22.1 x 4.7 cm
* Waga: max. 1.04 kg
* Powinno posiadać solidną metalową obudowę
* Temperatura pracy: od -20C do 85C,
* Praca w warunkach wilgotności: 10 do 90%,

Wymagania gwarancyjne i serwisowe

- zgodnie z wymaganiami określonymi w rozdziale V podpunkt 2.4.

* 1. Antena sektorowa WLAN 2,4 GHz MIMO (38 szt.)

**Cecha J**

Wymagania techniczne

częstotliwość : 2400-2500 MHz

impedancja: 50 OHm

VSWR : < 1.5

Polaryzacja: pozioma/pionowa

Minimalny zysk : 14 dBi

separacja przód/tył : > 30 dBi

separacja polaryzacji : > 20 dBi

wymiary : 340x194x25 mm

złącze: N żeńska

Wymagania gwarancyjne i serwisowe

- anteny powinny być objęte 36-miesięczną gwarancją producenta

* 1. Antena sektorowa WLAN 5 GHz MIMO (38 szt.)

**Cecha K**

Wymagania techniczne

częstotliwość : 5150-5850 MHz

impedancja: 50 OHm

VSWR: < 2.0

Polaryzacja: pozioma/pionowa

zysk : 17 dBi

separacja przód/tył : > 26 dBi

separacja polaryzacji: > 44 dBi

wymiary : 451x227x40 mm

złącze: N żeńska

Wymagania gwarancyjne i serwisowe

- anteny powinny być objęte 36-miesięczną gwarancją producenta

1. **Wyposażenie Głównego Węzła Dystrybucyjnego i Centrum Zarządzania siecią szerokopasmową.**

* 1. Adaptacja pomieszczenia Centrum Zarządzania siecią szerokopasmową

Planowane jest wykorzystanie pomieszczenia na parterze budynku Urzędu Gminy Bojanów na potrzeby budowy Głównego Węzła Dystrybucyjnego oraz Centrum Zarządzania siecią.

Zakres prac adaptacyjnych będzie się składał:

a) Robót budowlanych związanych z adaptacją pomieszczenia a w szczególności:

- dostawie i osadzeniu drzwi antywłamaniowych w celu fizycznego zabezpieczenia pomieszczenia

- montażu klimatyzatora

- montażu 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

- wykonać miejscowej szyny wyrównawczej oraz jej połączeniu przewodem LgYżo fi 16 mm z główną szyną uziemienia budynku

b) Instalacji systemu kontroli dostępu ACC w pomieszczeniu Serwerowni

Wymagania ogólne

* 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 obecności (czujka ruchu)

- Czujnik zbicia szkła

- Czujnik dymu

- 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.

.

* 1. Przełącznik rdzeniowy (min. 1 szt.)

**Cecha L**

Wymagania techniczne:

* Powinno być oparte o urządzenie o zamkniętej konfiguracji, wysokości 1 RU.
* Urządzenie powinno posiadać przynajmniej 128MB pamięci DRAM oraz 64MB pamięci Flash
* Urządzenie powinno obsłużyć 8000 adresów MAC
* Urządzenie powinno posiadać tzw. Switching Fabric o wydajności co najmniej 50 Gbps oraz przepustowość co najmniej 38,7 Mpps
* Urządzenie powinno posiadać co najmniej 24 portów Gigabit Ethernet w standardzie 10/100/1000BaseT plus dwa porty typu uplink Small Form-Factor Plugable (SFP) pozwalające na instalację wkładek z portami Gigabit Ethernet 1000BASE-T, 1000BASE-SX, 1000BASE-ZX, 1000BASE LX/LH.
* Urządzenie powinno posiadać wsparcie dla co najmniej 64 sieci VLAN oraz 4000 VLAN ID.
* Urządzenie powinno mieć wsparcie protokołów sieciowych zgodnie ze standardami:
  + IEEE 802.1x
  + IEEE 802.1s
  + IEEE 802.1w
  + IEEE 802.3x full duplex na portach 10BASE-T, 100BASE-TX oraz 1000BASE-T
  + IEEE 802.3ad
  + IEEE 802.1D
  + IEEE 802.1p
  + IEEE 802.1Q
  + IEEE 802.3 10BASE-T
  + IEEE 802.3u 100BASE-TX
  + IEEE 802.3z 1000BASE-X
  + IEEE 802.3ab 100BASE-T
* Urządzenie powinno wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:

1. Mechanizm zapewnienia jakości usług CoS
2. Mechanizm kolejkowania Shaped Round Robin (SSR).

* Urządzenie powinno wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:

1. Możliwość uzyskania dostępu do urządzenia przez SSHv2 i SNMPv3
2. Możliwość autoryzacji prób logowania do urządzenia za pomocą serwerów RADIUS i TACACS+
3. Możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. protected ports) z pozostawieniem możliwości komunikacji z portem nadrzednym (designated port) lub funkcjonalność Private VLAN Edge
4. możliwość tworzenia portów monitorujących, pozwalających na kopiowanie na port monitorujący ruchu z innego dowolnie wskazanego portu lub sieci VLAN z lokalnego przełącznika
5. ochrona przed rekonfiguracją struktury topologii Spanning Tree spowodowana przez niepowołane i nieautoryzowane urządzenie sieciowe
6. min. 5 poziomów uprawnień do zarządzania urządzeniem (z możliwością konfiguracji zakresu dostępnych funkcjonalności i komend)
7. współpraca z systemami kontroli dostępu do sieci typu NAC, NAP itp.

* Powinno wspierać obsługę ruchu multicast z wykorzystaniem IGMPv3 oraz możliwość utworzenia co najmniej 255 grup
* Urządzenie powinno umożliwiać grupowanie portów w jeden kanał logiczny zgodnie z LACP
* Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line. Tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej powinno być możliwe uruchomienie urządzenia z nowa konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.
* Urządzenie powinno mieć możliwość ochrony przed rekonfiguracją struktury topologii Spanning Tree spowodowana przez niepowołane i nieautoryzowane urządzenie sieciowe.
* Urządzenie powinno być zarządzane przy pomocy bezpłatnej aplikacji graficznej dostarczonej przez producenta.
* Urządzenie powinno obsługiwać tzn.: Jumbo Frames
* Urządzenie powinno mieć możliwość montażu w szafie 19”, a jego obudowa powinna być wykonana z metalu.

Wymagania gwarancyjne i serwisowe

- zgodnie z wymaganiami określonymi w rozdziale V podpunkt 2.4.

* 1. Router brzegowy (1 szt.)

**Cecha M**

Wymagania funkcjonalne i techniczne

*Wyposażenie*

* Urządzenie musi być routerem modularnym wyposażonym w minimum 3 interfejsy Gigabit Ethernet 10/100/1000 dla realizacji połączenia do sieci LAN.
* Urządzenie musi być wyposażone w minimum 256MB pamięci Flash i mieć możliwość rozbudowy do co najmniej 4GB
* Urządzenie musi być wyposażone w minimum 512MB pamięci RAM z możliwością rozbudowy do co najmniej 2,5GB
* Urządzenie musi być wyposażone w minimum dwa porty USB. Porty muszą pozwalać na podłączenie zewnętrznych pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych oraz pełnić funkcję konsoli szeregowej.
* Urządzenie musi być dostarczone z kablami pozwalającymi na podłączenie konsoli szeregowej.

*Architektura*

* Musi być urządzeniem modularnym posiadającym możliwość instalacji co najmniej:
  1. 4 modułów sieciowych z interfejsami
  2. 1 modułu usługowego z interfejsami. Moduły usługowe powinny mieć możliwość wyłączenia w celu oszczędzania energii elektrycznej
  3. 1 wewnętrznego modułu usługowego
  4. 2 modułów z układami DSP. Moduły DSP powinny mieć możliwość wyłączenia w celu oszczędzania energii elektrycznej
* Musi posiadać zainstalowany wewnętrzny sprzętowy moduł akceleracji szyfrowania DES/3DES/AES
* Musi posiadać możliwość skonfigurowania bezpośredniej komunikacji pomiędzy wybranymi modułami usługowymi z pominięciem głównego procesora.
* Musi posiadać wszystkie interfejsy „aktywne”. Nie dopuszcza się stosowania kart, w których dla aktywacji interfejsów potrzebne będą dodatkowe licencje lub klucze aktywacyjne i konieczne wniesienie opłat licencyjnych. Np. niedopuszczalne jest stosowanie karty 4-portowej gdzie aktywne są 2 porty, a dla uruchomienia pozostałych konieczne jest wpisanie kodu, który uzyskuje się przez wykupienie licencji na użytkowanie pozostałych portów.
* Sloty urządzenia przewidziane pod rozbudowę o dodatkowy moduł usługowy muszą mieć możliwość obsadzenia modułami:
  1. z portami szeregowymi – o gęstości co najmniej 4 porty na moduł
  2. z interfejsem ISDN BRI (styk S/T) - o gęstości co najmniej 8 portów na moduł
  3. z przełącznikiem Ethernet - o gęstości co najmniej 16 portów na moduł
  4. content engine
  5. Intrusion Detection System
  6. Analizatora sieciowego
* Sloty urządzenia przewidziane pod rozbudowę o dodatkową kartą sieciową muszą mieć możliwość obsadzenia kartami:
  1. z portami szeregowymi – o gęstości co najmniej 2 porty na moduł
  2. ze zintegrowanym modemem ADSL - o gęstości co najmniej 1 port na moduł
  3. ze zintegrowanym modemem SHDSL - o gęstości co najmniej 1 port na moduł
  4. z interfejsem ISDN BRI (styk S/T) - o gęstości co najmniej 1 port na moduł
  5. z przełącznikiem Ethernet - o gęstości co najmniej 4 portów na moduł
* Sloty urządzenia przewidziane pod rozbudowę o moduł z układami DSP muszą mieć możliwość obsadzenia modułami:
  1. gęstości nie mniejszej niż 128 kanałów
  2. Pozwalającymi na dynamiczne alokowanie DSP do różnych zadań (osługa interfejsów głosowych, trancoding, conferencing) z granulacją do 1 DSP.
  3. Posiadających wsparcie dla usług wideo
* Oczekiwana wydajność proponowanego rozwiązania z włączonymi usługami nie może być mniejsza niż 35Mbit/s

*Oprogramowanie - funkcjonalność*

* Oprogramowanie routera musi umożliwiać rozbudowę o dodatkowe funkcjonalności bez konieczności instalacji nowego oprogramowania. Nowe zbiory funkcjonalności muszą być dostępne poprzez wprowadzenie odpowiednich licencji.
* Musi posiadać obsługę protokołów routingu IP BGPv4, OSPFv3, IS-IS, RIPv2 oraz routingu multicastowego PIM (Sparse i Dense) oraz routing statyczny
* Protokół BGP musi posiadać obsługę 4 bajtowych ASN
* Musi posiadać wsparcie dla funkcjonalności Policy Based Routing
* Musi posiadać wsparcie dla mechanizmów związanych z obsługą ruchu multicast: IGMP v3, IGMP Snooping, PIMv1, PIMv2
* Musi posiadać obsługę protokołu IGMPv3
* Musi posiadać wsparcie dla protokołu DVMRP
* Musi obsługiwać mechanizm Unicast Reverse Path Forwarding (uRPF)
* Musi obsługiwać tzw.routing między sieciami VLAN w oparciu o trunking 802.1Q
* Musi obsługiwać IPv6 w tym ICMP dla IPv6
* Musi zapewniać obsługę list kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, opcje IP, flagi TCP, oraz o wartości TTL
* Musi zapewniać mechanizmy korelacji zdarzeń związanych z filtracją za pomocą list kontroli dostępu dla syslog (np. za pomocą etykiety przypisanej do określonego wpisu na listach kontroli dostępu lub skrót MD5 generowany przez router)
* Musi posiadać obsługę NAT dla ruchu IP unicast i multicast oraz PAT dla ruchu IP unicast
* Mechanizm NAT musi zapewniać wsparcie dla H.224/H.245
* Musi posiadać wsparcie dla protokołów WCCP i WCCPv2
* Musi posiadać obsługę wirtualnych instancji routingu (VRF) - co najmniej 15 instancji VRF
* Musi być w stanie obsłużyć 20 000 wpisów w tablicach VRF (sumaryczna wartość dla wszystkich VRF)
* Musi posiadać obsługę mechanizmu DiffServ
* Musi mieć możliwość tworzenia klas ruchu oraz oznaczanie (Marking), klasyfikowanie i obsługę ruchu (Policing, Shaping) w oparciu o klasę ruchu.
* Musi zapewniać obsługę mechanizmów kolejkowania ruchu:
  1. z obsługą kolejki absolutnego priorytetu
  2. ze statyczną alokacją pasma dla typu ruchu
  3. WFQ
* Musi obsługiwać mechanizm WRED
* Musi obsługiwać protokoł RSVP
* Musi obsługiwać mechanizm Generic Traffic Shaping
* Musi obsługiwać mechanizm ograniczania pasma dla określonego typu ruchu
* Musi obsługiwać protokół GRE oraz zapewnieniać mechnizm honorowania IP Precendence dla ruchu tunelowanego.
* Musi obsługiwać protokół NTP
* Musi obsługiwać DHCP w zakresie Client, Server
* Musi posiadać obsługę tzw. First Hop Redundancy Protocol (takiego jak HSRP, GLBP, VRRP lub odpowiednika)
* Musi posiadać obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS lub TACACS+
* Musi posiadać funkcjonalność firewall (w trybie routed oraz transparent)
* Musi posiadać funkcjonalność Intrusion Prevention System
* Musi posiadać funkcjonalność Content Filtering
* Musi posiadać możliwość szyfrowania połączeń z wykorzystaniem algorytmów DES/3DES

*Zarządzanie i konfiguracja*

* Musi być zarządzalne za pomocą SNMPv3
* Musi mieć możliwość eksportu statystyk ruchowych za pomocą protokołu Neftflow/JFlow lub odpowiednika
* Musi być konfigurowalne za pomocą interfejsu linii poleceń (ang. Command Line Interface – CLI)
* Plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) musi pozwalać na edycję w trybie off-line, tzn. musi być możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym komputerze. Po zapisaniu konfiguracji w pamiąci nieulotnej powinno być możliwe uruchomienie urządzenia z nowa konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.

*Obudowa*

* Musi być wykonana z metalu. Ze względu na różne warunki w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowie plastikowej
* Musi mieć możliwość montażu w szafie 19”

*Zasilanie*

* Urządzenie musi mieć możliwość zasilania ze źródeł zmiennoprądowych 230V (zasilacza AC) oraz stałoprądowych (zasilacze DC)
* Urządzenie musi posiadać wbudowany zasilacz umożliwiający zasilanie prądem przemiennym 230V
* Urządzenie musi umożliwiać doprowadzenie zasilania do portów Ethernet (tzw. inline-power) - w modułach sieciowych dostępnych do urządzenia
* Urządzenie musi mieć możliwość instalacji zewnętrznego zasilacza redundantnego

Wymagania gwarancyjne i serwisowe

- zgodnie z wymaganiami określonymi w rozdziale V podpunkt 2.4.

* 1. Urządzenie bezpieczeństwa sieciowego (1 szt.)

**Cecha N**

Wymagania techniczne

* Urządzeniu musi realizować funkcję firewall.
* Przepustowość firewall’a na poziomie 300 Mbps.
* Przepustowość dla ruchu szyfrowanego 3DES/AES: 170 Mbps.
* Maksymalna liczba kanałów VPN: 250.
* Maksymalna liczba sesji: 130 000.
* Maksymalna liczba sesji na sekundę:  9000.
* Pamięć RAM min 256 MB.
* Pamięć flash min 64 MB.
* Pięć zintegrowanych interfejsów Ethernet, w tym co najmniej dwa GigabitEthernet 10/100/1000.
* Jeden port konsoli, jeden port do transmisji szeregowej, dwa porty USB.
* Obsługa protokołów RIP, OSPF, PIM, EIGRP.
* Wbudowany serwer DHCP.
* Obsługa IPv6.
* Możliwość definiowania przydziału pasma i priorytetów dla wybranych klas ruchu.
* Możliwość pracy w trybie transparentnym w warstwie 2
* Funkcje translacji adresów NAT, PAT.
* Analiza protokołów HTTP, FTP, ESMTP, DNS, SNMP, ICMP, SQL\*Net, NFS, H.323, SIP, SCCP, MGCP, RTSP, TAPI i JTAPI, GPRS Tunneling Protocol (GTP), LDAP, ILS, RPC.
* Sprawdzanie zgodności wykorzystywania analizowanych protokołów z procedurami RFC.
* Dogłębna analiza sesji HTTP.
* Kontrola ruchu typu pee-to-peer, instant messeging (IM) i aplikacji tunelowanych poprzez port 80, analiza Multipurpose Internet Mail Extensions (MIME).
* Obsługa do 100 sieci VLAN w standardzie 802.1Q.
* Urządzenie musi mieć slot na jeden z poniższych modułów rozszerzeń:
  + 1. moduł ochrony antywirusowej,
    2. moduł IPS z pamięcią RAM 1 GB i flash 256 MB
    3. moduł z czterema portami GigabitEthernet
* Urządzenie musi umożliwiać konfigurację 2 wirtualnych urządzeń firewall, a po wykupieniu odpowiedniej licencji, do 5 wirtualnych firewall.
* Firewall powinien zapewniać uwierzytelnianie w oparciu o Active Direktory, SecureID, Radius, LDAP.
* Możliwość pracy redundantnej w trybie Active/Standby i Active/Active.
* Zarządzanie za pomocą bezpiecznego połączenia HTTPS, SSH oraz lokalnie za pomocą kabla szeregowego.
* Obsługa certyfikatów X.509 (SCEP, PKCS #7, #10, #12).
* Dołączone oprogramowanie klienta VPN .
* Certyfikaty ICSA Firewall, ICSA IPSec.
* Obudowa umożliwiająca instalację w szafie rack 19”, wysokość nie przekraczająca 1U.

Wymagania gwarancyjne i serwisowe

- zgodnie z wymaganiami określonymi w rozdziale V podpunkt 2.4.

* 1. Kontroler sieci bezprzewodowej WLAN (1 szt.)

**Cecha O**

Wymagania techniczne i funkcjonalne:

*Wymagania dla systemu bezprzewodowego WiFi:*

* obsługa standardów 802.11a/b/g/e/h/i
* obsługa standardu IEEE 802.11n 2.0
* automatyczne zarządzanie pasmem radiowym
* automatyczna adaptacja do zmian środowiska radiowego w czasie rzeczywistym
* optymalizacja mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia, eliminacja zakłóceń między kanałami)
* dynamiczne przydzielanie kanałów radiowych
* wykrywanie, eliminacja i unikanie interferencji
* równoważenie obciążenia punktów dostępowych (możliwość automatycznego rozkładania asocjacji klientów pomiędzy różne punkty dostępowe)
* obsługa DynamicFrequencySelection (DFS) i Transmit Power Control (TPC) zgodnie z decyzją ECC/DEC(04)08
* obsługa mechanizmów bezpieczeństwa
  + 802.11i, WPA2, WPA, WEP
  + 802.1x z EAP (PEAP, EAP-TLS, EAP-FAST, EAP-TTLS, EAP-SIM)
  + możliwość kreowania różnych polityk bezpieczeństwa w ramach pojedynczego SSID oraz pomiędzy SSID
  + możliwość rozgłaszania lub ukrycia poszczególnych SSID
  + obsługa serwerów autoryzacyjnych (RADIUS lub TACACS+, LDAP),
  + możliwość lokalnej definicji profili użytkowników
  + możliwość profilowania użytkowników (przydział sieci VLAN, przydział list kontroli dostępu (ACL))
  + współpraca z mechanizmami zaawansowanej kontroli dostępu do sieci (typu NAC, NAP lub równoważne) – wymuszanie polityki dostępu na poziomie kontrolera
  + uwierzytelnianie punktów dostępowych do kontrolera za pomocą certyfikatów X.509
  + ochrona kryptograficzna ruchu kontrolnego pomiędzy kontrolerem a punktami dostępowymi (AES)
  + uwierzytelnianie ramek zarządzania 802.11 w oparciu o technologie kryptograficzne (wykrywanie podszywania się punktów dostępowych pod adresy infrastruktury)
* wykrywanie „obcych” punktów dostępowych
* monitorowanie pasma radiowego równocześnie z obsługą danych
* współpraca z mechanizmami lokalizacyjnymi oprogramowania do zarządzania)
* wbudowany system IDS wykrywający ataki typowe dla środowisk WLAN
* współpraca z zewnętrznymi systemami IDS/IPS (możliwość sterowania systemem dostępu bezprzewodowego przez sondy IDS/IPS – de asocjacja użytkownika w przypadku wykrycia ataku)
* obsługa mechanizmów QoS (802.1p, WMM TSpec, kontrola pasma per użytkownik) i VoWLAN (Voice over WLAN)
* obsługa mobilności (roaming-u) użytkowników w warstwie 2 i 3 z cache’owaniem danych autoryzacyjnych i kluczy (dla WEP, WPA, WPA2)
* obsługa dostępu gościnnego:
  + przekierowanie użytkowników określonych SSID do strony logowania (z możliwością personalizacji strony per SSID)
  + możliwość kreowania użytkowników za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta
  + możliwość konfiguracji dedykowanego kontrolera do obsługi ruchu gości – całość ruchu z SSID dostępu gościnnego zebranego na pozostałych kontrolerach musi być przesyłana do tego kontrolera (umieszczonego w publicznej części sieci) w sposób zapewniający logiczną separację od ruchu wewnętrznego
* obsługa IPv4 i IPv6 (w ramach pojedynczego SSID)
* hierarchizacja uprawnień administratorów systemu
* możliwość rozszerzenia funkcjonalności o funkcje lokalizacyjne (możliwość lokalizowania i śledzenia urządzeń końcowych, obcych AP i klientów)

Wszystkie elementy z których zbudowany ma być system dostępu bezprzewodowego (kontroler, punkt dostępowy) muszą być tego samego producenta.

*Wymagania dla kontrolera sieci bezprzewodowej:*

* zarządzanie min. 50 punktami dostępowymi w trybie lekkim z możliwością licencyjnej rozbudowy systemu do 500 punktów dostępowych
* min. 8 styków definiowanych przez moduły typu SFP zgodnymi ze standardami 1000BaseT, 1000Base-SX oraz 1000Base-LH z możliwością agregacji pasma - wymagane wyposażenie kontrolera w min. 2 moduły SFP 1000Base-T
* dedykowany port Ethernet 10/100/1000 do zarządzania out-of-band
* dedykowany port dla konsoli szeregowej
* obsługa 802.1q
* możliwość zapewnienia redundancji
* zarządzanie przez HTTPS, SNMPv3, SSH, port konsoli szeregowej
* zgodność ze standardami:

- SNMP v1, v2c, v3

- RFC 854 Telnet

- RFC 1155 Management Information for TCP/IP-Based Internets

- RFC 1156 MIB

- RFC 1157 SNMP

- RFC 1213 SNMP MIB II

- RFC 1350 TFTP

- RFC 1643 Ethernet MIB

- RFC 2030 SNTP

- RFC 2616 HTTP

- RFC 2665 Ethernet-Like Interface types MIB

- RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions

- RFC 2819 RMON MIB

- RFC 2863 Interfaces Group MIB

- RFC 3164 Syslog

- RFC 3414 User-Based Security Model (USM) for SNMPv3

- RFC 3418 MIB for SNMP

- RFC 3636 Definitions of Managed Objects for IEEE 802.3 MAUs

- RFC 768 UDP

- RFC 791 IP

- RFC 792 ICMP

- RFC 793 TCP

- RFC 826 ARP

- RFC 1122 Requirements for Internet Hosts

- RFC 1519 CIDR

- RFC 1542 BOOTP

- RFC 2131 DHCP

- WPA

- IEEE 802.11i (WPA2, RSN)

- RFC 1321 MD5 Message-Digest Algorithm

- RFC 1851 The ESP Triple DES Transform

- RFC 2104 HMAC: Keyed Hashing for Message Authentication

- RFC 2246 TLS Protocol Version 1.0

- RFC 2401 Security Architecture for the Internet Protocol

- RFC 2403 HMAC-MD5-96 within ESP and AH

- RFC 2404 HMAC-SHA-1-96 within ESP and AH

- RFC 2405 ESP DES-CBC Cipher Algorithm with Explicit IV

- RFC 2406 IPSec

- RFC 2407 Interpretation for ISAKMP

- RFC 2408 ISAKMP

- RFC 2409 IKE

- RFC 2451 ESP CBC-Mode Cipher Algorithms

- RFC 3280 Internet X.509 PKI Certificate and CRL Profile

- RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPSec

- RFC 3686 Using AES Counter Mode with IPSec ESP

- IEEE 802.1X

- RFC 2716 PPP EAP-TLS

- RFC 2865 RADIUS Authentication

- RFC 2866 RADIUS Accounting

- RFC 2867 RADIUS Tunnel Accounting

- RFC 2869 RADIUS Extensions

- RFC 3576 Dynamic Authorization Extensions to RADIUS

- RFC 3579 RADIUS Support for EAP

- RFC 3580 IEEE 802.1X RADIUS Guidelines

- RFC 3748 ExtensibleAuthenticationProtocol

* dostarczone licencje muszą umożliwiać uruchomienie wszystkich funkcjonalności systemu. Nie jest dopuszczalne dodatkowe licencjonowanie poszczególnych funkcjonalności (np. związanych z bezpieczeństwem)
* możliwość zastosowania redundantnego zasilacza AC
* możliwość instalacji w szafie rack 19”
* Pobór mocy: max. 115 Watt,
* oznaczenie CE

Wymagania gwarancyjne i serwisowe

- zgodnie z wymaganiami określonymi w rozdziale V podpunkt 2.4.

* 1. Zasilacz awaryjny UPS 3000 VA (wraz bateriami) (min. 1 szt.)

**Cecha P**

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 producenta.

* 1. Szafa 42U z wyposażeniem (1 szt.)

**Cecha R**

Wyposażenie

Szafa serwerowa 42U szer:800 głeb:1000

Drzwi tylne i przednie 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

* 1. Serwery i urządzenia dodatkowe

Wymagania techniczne (sprzętowe oraz systemowe):

* + 1. Serwer LMS (1 szt.)

**Cecha 1**

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa komponentu | Wymagane minimalne parametry techniczne |
| Serwer | | |
|  | Płyta główna | dedykowana do pracy w serwerach, posiadająca moduł TPM i dwa gniazda na procesory, wyprodukowana przez producenta serwera i oznaczona jego znakiem firmowym.  Dwa sloty PCI Express. Minimum jeden slot PCIe x16 pozwalający na instalację karty pełnej wysokości |
|  | Chipset | Rekomendowany przez producenta procesora |
|  | Procesor | Jeden procesor czterordzeniowy, dedykowany do pracy w serwerach, o wydajności równoważnej lub wyższej procesorowi Intel® Xeon® E5504  Dopuszcza się zaoferowania serwerów z większą liczbą procesorów, przy założeniu że oferowany serwer z większą liczbą procesorów będzie miał wydajność równa lub większą od wymaganej.  W przypadku użycia przez oferenta testów wydajności Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testów oferent musi dostarczyć zamawiającemu oprogramowanie testujące, oba równoważne porównywalne serwery oraz dokładny opis użytych testów wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego.  Maksymalny pobór mocy przez jeden procesor wynosi: 80 W.  Maksymalna liczba obsługiwanych procesorów wynosi 2 |
|  | Pamięć RAM | 4GB DDR3 ,możliwość instalacji w serwerze do 144GB pamięci RAM |
|  | Dysk twardy | Dwa dyski hot-plug SATA o pojemności min. 500GB, możliwość rozbudowy do min 4 dysków w serwerze |
|  | Kontroler | Kontroler macierzowy PCI Express 2.0 x8 SATA/SAS wyposażony w pamięć cache 256 MB oraz baterię podtrzymującą napięcie w razie braku zasilania, zapewniający obsługę 4 napędów dyskowych SATA/SAS oraz obsługujący poziomy RAID 0/1/1+0/5 |
|  | Karta graficzna | Zintegrowana z płytą główną, 32MB |
|  | Karta sieciowa | 2 x Gigabit Ethernet 10/100/1000, 1x dedykowany port zarządzania |
|  | Porty | 2 porty RJ-45 LAN,  1 port RJ-45 Management,  5 portów USB ( w tym 1 port wewnętrzny ) ,  1 port VGA (15-pin video),  1 port szeregowy. |
|  | Klawiatura | Klawiatura USB pełnowymiarowa – trwale oznaczona logo producenta jednostki centralnej |
|  | Mysz | Mysz optyczna USB z dwoma klawiszami oraz rolką (scroll) – trwale oznaczona logo producenta |
|  | Napęd optyczny | Nagrywarka DVD +/-RW |
|  | Obudowa | Obudowa o wysokości maksymalnie 1U dedykowana do montażu w szafie rack 19" z zestawem szyn mocujących  Jeden zasilacz o mocy minimum 500W |
|  | Obsługiwane systemy operacyjne | MS Windows Server 2003, MS Windows Server 2008, Linux RedHat, Linux SUSE |
|  | Standardy branżowe | ACPI V2.0, PCI 2.2, PXE, WOL, Microsoft® Logo certifications, IPMI 2.0, SMASH CLP, DCMI 1.0 |
|  | Zarządzanie | Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS).  Karta ta musi umożliwiać również przeje zdalnej konsoli graficznej i podłączania wirtualnych napędów DVD i FDD  Wszystkie powyższe funkcjonalności muszą być dostępne bez konieczności dokładania dodatkowych kart sprzętowych w sloty PCI-X/PCI-Express.  Pozostałe wymagania:  Zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego .Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe PCI. |
| Oprogramowanie | | |
|  | System LMS | Wymagana jest dostawa oraz konfiguracja specjalizowanego oprogramowania (wraz z wszelkimi niezbędnymi licencjami) tworzącego system zarządzania oraz administracji usługami dostępu do Internetu i użytkownikami sieci (zgodnie z wymaganiami określonymi w pkt. 4.7.1.1 ) |
| Gwarancja | | |
|  | Gwarancja | 3 lata w miejscu eksploatacji  Oferent musi posiadać autoryzację producenta serwera – dokumenty potwierdzające załączyć do oferty.  Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta – dokumenty potwierdzające załączyć do oferty.  Oświadczenie producenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem gwarancyjnym. |

4.7.1.1. 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, hasła dostępu, data zakupu, okres gwarancji, ilość portów, 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 dostępowych klienta, generowanie oraz przetrzymywanie dokumentów klienta (np. umowa, protokóły)
* moduł finansowo-ksiegowy z fakturowaniem oraz automatycznym naliczaniem należności
* 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 oraz zliczanie ruchu urządzeń w oparciu o dane z bazy danych SQL
  + 1. Serwer „TrafficManager” (1 szt.)

**Cecha 2**

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa komponentu | Wymagane minimalne parametry techniczne |
| Serwer | | |
|  | Płyta główna | dedykowana do pracy w serwerach, posiadająca moduł TPM i dwa gniazda na procesory, wyprodukowana przez producenta serwera i oznaczona jego znakiem firmowym.  Dwa sloty PCI Express. Minimum jeden slot PCIe x16 pozwalający na instalację karty pełnej wysokości |
|  | Chipset | Rekomendowany przez producenta procesora |
|  | Procesor | Jeden procesor czterordzeniowy, dedykowany do pracy w serwerach, o wydajności równoważnej lub wyższej procesorowi Intel® Xeon® E5504  Dopuszcza się zaoferowania serwerów z większą liczbą procesorów, przy założeniu że oferowany serwer z większą liczbą procesorów będzie miał wydajność równa lub większą od wymaganej.  W przypadku użycia przez oferenta testów wydajności Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testów oferent musi dostarczyć zamawiającemu oprogramowanie testujące, oba równoważne porównywalne serwery oraz dokładny opis użytych testów wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego.  Maksymalny pobór mocy przez jeden procesor wynosi: 80 W.  Maksymalna liczba obsługiwanych procesorów wynosi 2 |
|  | Pamięć RAM | 4GB DDR3 ,możliwość instalacji w serwerze do 144GB pamięci RAM |
|  | Dysk twardy | Dwa dyski hot-plug SATA o pojemności min. 500GB, możliwość rozbudowy do min 4 dysków w serwerze |
|  | Kontroler | Kontroler macierzowy PCI Express 2.0 x8 SATA/SAS wyposażony w pamięć cache 256 MB oraz baterię podtrzymującą napięcie w razie braku zasilania, zapewniający obsługę 4 napędów dyskowych SATA/SAS oraz obsługujący poziomy RAID 0/1/1+0/5 |
|  | Karta graficzna | Zintegrowana z płytą główną, 32MB |
|  | Karta sieciowa | 2 x Gigabit Ethernet 10/100/1000, 1x dedykowany port zarządzania |
|  | Porty | 2 porty RJ-45 LAN,  1 port RJ-45 Management,  5 portów USB ( w tym 1 port wewnętrzny ) ,  1 port VGA (15-pin video),  1 port szeregowy. |
|  | Klawiatura | Klawiatura USB pełnowymiarowa – trwale oznaczona logo producenta jednostki centralnej |
|  | Mysz | Mysz optyczna USB z dwoma klawiszami oraz rolką (scroll) – trwale oznaczona logo producenta |
|  | Napęd optyczny | Nagrywarka DVD +/-RW |
|  | Obudowa | Obudowa o wysokości maksymalnie 1U dedykowana do montażu w szafie rack 19" z zestawem szyn mocujących  Jeden zasilacz o mocy minimum 500W |
|  | Obsługiwane systemy operacyjne | MS Windows Server 2003, MS Windows Server 2008, Linux RedHat, Linux SUSE |
|  | Standardy branżowe | ACPI V2.0, PCI 2.2, PXE, WOL, Microsoft® Logo certifications, IPMI 2.0, SMASH CLP, DCMI 1.0 |
|  | Zarządzanie | Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS).  Karta ta musi umożliwiać również przeje zdalnej konsoli graficznej i podłączania wirtualnych napędów DVD i FDD  Wszystkie powyższe funkcjonalności muszą być dostępne bez konieczności dokładania dodatkowych kart sprzętowych w sloty PCI-X/PCI-Express.  Pozostałe wymagania:  Zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego .Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe PCI. |
| Oprogramowanie | | |
|  | System TrafficManager | Wymagana jest dostawa oraz konfiguracja specjalizowanego oprogramowania (wraz z wszelkimi niezbędnymi licencjami) pełniącego role bramy dla klienckich sieci dostępowych (zgodnie z wymaganiami określonymi w pkt. 4.7.2.1) |
| Gwarancja | | |
|  | Gwarancja | 3 lata w miejscu eksploatacji  Oferent musi posiadać autoryzację producenta serwera – dokumenty potwierdzające załączyć do oferty.  Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta – dokumenty potwierdzające załączyć do oferty.  Oświadczenie producenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem gwarancyjnym. |

4.7.2.1. Wymagania ogólne dotyczące zainstalowanego oprogramowania:

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.



Wymagania funkcjonalne systemu „TrafficManager”:

Oprogramowanie musi posiadać następujące cechy i funcje:

* 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
  + 1. Serwer pamięci masowej (1 szt.)

**Cecha 3**

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa komponentu | Wymagane minimalne parametry techniczne |
| Serwer | | |
|  | System operacyjny | Embeded Linux |
|  | Procesor | Intel Atom 1.6 GHz |
|  | Pamięć | Flash 128MB (DOM), RAM 1GB DDRII |
|  | Dysk twardy | Dostępne 4 kieszenie hot-swap z możliwością zablokowania  Zainstalowane 4 dyski hot-swap dedykowane do pracy w serwerach, każdy po 2000GB SATA II |
|  | Kontroler | RAID 0/ 1/ 5/ 6/ 5+ hot spare, JBOD |
|  | System plików | Internal HDD: EXT3, EXT4  External HDD: EXT3, EXT4, NTFS, FAT32, HFS+ |
|  | Karta sieciowa | 2 x Gigabit LAN, wbudowana usługa iSCSI |
|  | Porty | 3 x USB 2.0 |
|  | Obudowa | Obudowa o wysokości maksymalnie 1U dedykowana do montażu w szafie rack 19" z zestawem szyn mocujących  Dwa zasilacze (redundant) |
|  | Obsługiwane systemy operacyjne | Microsoft Windows 98/ ME/ NT/ 2000/ XP/ 2003/ Vista; 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) |
|  | Przyciski | Power, USB One-Touch-Backup, reset |
|  | Zarządzanie | ograniczenie dostępnej pojemności dysku dla użytkownika, Windows AD, zarządzanie kontami użytkowników (maksymalnie 4096 użytkowników), zarządzanie grupą użytkowników (maksymalnie 512 grup), tworzenie zestawów użytkowników |
| Oprogramowanie | | |
|  | System backupu | Acronis Backup & Recovery 10 Advanced Server lub równoważny – 2 licencje |
| Gwarancja | | |
|  | Gwarancja | 3 lata w miejscu eksploatacji |

* + 1. Stacja do zarządzania (1 szt.)

**Cecha 4**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Lp. | | Nazwa atrybutu | Wymagane minimalne | |
| Komputer stacjonarny | | | | |
|  | Wydajność | | | Procesor klasy x86, dedykowany do pracy w komputerach stacjonarnych uzyskujący przy pracy w nominalnych warunkach w teście Passmark CPU Mark wynik min. 2000 punktów (wynik zaproponowanego procesora musi znajdować sie na stronie <http://www.cpubenchmark.net>, zaś wydruk potwierdzenia dołączony do oferty) |
|  | Pamięć | | | min. 4GB pamięci operacyjnej z możliwością rozbudowy do 16GB  min. 500GB pamięci masowej SATAII |
|  | Grafika | | | min. 512MB pamięci dedykowanej, wspierająca technologię Microsoft DirectX 10, OpenGL 2.01, Shader Model 4.0, obsługująca dwa monitory o rozdzielczościach do 2560x1600 |
|  | Napędy wbudowane | | | Nagrywarka DVD +/-RW wraz z oprogramowaniem do nagrywania płyt  Czytnik kart multimedialnych 22-in-1 |
|  | Funkcjonalność BIOS | | | możliwość odczytania: wersji BIOS; oraz niezamazywalnej informacji zawierającej nazwę oraz numer seryjny komputera,  - możliwość skonfigurowania hasła „Power On”,  - możliwość ustawienia hasła dostępu do BIOSu (administratora),  - możliwość blokady portów USB, COM i Centronics;  - możliwość wyłączenia w BIOS-ie portów USB;  - możliwość wyłączenia w BIOS-ie portu szeregowego;  - możliwość wyłączenia w BIOS-ie portu równoległego;  - możliwość kontroli sekwencji boot-owania;  - możliwość startu systemu z urządzenia USB |
|  | Funkcjonalność obudowy | | | - zasilacz o mocy min. 320W z aktywnym PFC i sprawności min. 89%  - możliwość zastosowania zabezpieczenia fizycznego w postaci linki metalowej lub kłódki (oczko w obudowie do założenia kłódki)  - możliwość zamontowania urządzeń (2x 5,25” zewnętrzne, 1x 3,5” zewnętrzne, 2x 3,5” wewnętrzne)  - przystosowanie do pracy w pozycji pionowej i dostępu do komponentów bez użycia narzędzi |
|  | Oprogramowanie | | | - System Microsoft Windows 7 Professional PL 32/64-bit, nie wymagający aktywacji za pomocą telefonu lub Internetu w firmie Microsoft. Dołączone nośniki z oprogramowaniem  - System diagnostyczny producenta komputera umożliwiający wykrywanie usterek z wyprzedzeniem  - Oprogramowanie producenta komputera do wykonania kopii bezpieczeństwa systemu operacyjnego i danych użytkownika na dysku twardym i dyskach zewnętrznych np. CD-ROM oraz ich odtworzenie po ewentualnej awarii systemu operacyjnego bez potrzeby jego reinstalacji;  - Oprogramowanie producenta komputera umożliwiające zdalną inwentaryzację sprzętu, monitorowanie stanu jego pracy, zmianę ustawień BIOS’u oraz aktualizację sterowników oraz BIOS’u;  - Wbudowana w płytę główną technologia zarządzania i monitorowania, która niezależnie od obecności systemu operacyjnego, powinna umożliwiać:  a) monitorowanie konfiguracji komponentów komputera - CPU, pamięć, HDD, wersje BIOS płyty głównej;  b) zdalną konfigurację BIOSu, zdalne uaktualnienie BIOSu;  c) zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego;  d) zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nieulotnej. |
|  | Certyfikaty i standardy | | | Wymagane są dokumenty poświadczające:  - Zgodność z oferowaną wersją systemu operacyjnego, potwierdzoną certyfikatem firmy Microsoft  - Certyfikat ISO9001 oraz ISO14001 dla producenta sprzętu  - Głośność jednostki centralnej mierzoną zgodnie z normą ISO 7779 oraz wykazaną zgodnie z normą ISO 9296 w pozycji obserwatora w trybie jałowym (IDLE) wynoszącą maksymalnie 27 dB  - 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 – do oferty należy dołączyć adres strony. |
|  | Wymagania dodatkowe | | | - Płyta główna zaprojektowana na zlecenie producenta jednostki centralnej komputera, opatrzona trwałym jego logo  - Min. 10 gniazd USB, w tym 4 z przodu obudowy  - Złącza video 1 x VGA DB-15, 1 x Display Port  - Porty audio: z tyłu obudowy 2 szt. (wejście i wyjście liniowe), z przodu obudowy 2 szt. (wyjście na słuchawki, wejście na mikrofon)  - Gniazdo RS232, Gigabit Ethernet, 2x PS/2  - Wolne sloty: 1 złącze PCI Express x16, 1 złącze PCI, 2 złącza PCI Express x1  - Klawiatura USB w układzie polski programisty, Mysz optyczna USB z dwoma klawiszami oraz rolką (scroll)  - Zintegrowany w płycie głównej aktywny układ zgodny ze standardem Trusted Platform Module (TPM v 1.2) |
| Monitor | | | | |
|  | Typ ekranu | | | Ekran ciekłokrystaliczny z matrycą typu TN 19” |
|  | Rozmiar plamki | | | 0,2835 mm |
|  | Jasność | | | 250 cd/m2 |
|  | Kontrast | | | 1000:1 |
|  | Kąty widzenia (pion/poziom) | | | 160/160 stopni |
|  | Czas reakcji matrycy | | | 5 ms |
|  | Rozdzielczość maksymalna | | | 1440 x 900 przy 60Hz |
|  | Częstotliwość odświeżania poziomego | | | 24 – 83 kHz |
|  | Częstotliwość odświeżania pionowego | | | 50 – 76 Hz |
|  | Podświetlenie | | | System podświetlenia CCFL |
|  | Bezpieczeństwo | | | Możliwość zastosowania zabezpieczenia fizycznego w postaci linki metalowej |
|  | Zużycie energii  Praca/spoczynek | | | max.29W / 2W |
|  | Złącze | | | 15-stykowe złącze D-Sub |
|  | Certyfikaty i standardy | | | TCO 03, ISO 13406-2 lub ISO 9241, EPEAT Silver, Energy Star |
|  | Głośniki | | | Stereo, przystosowane do integracji z obudową monitora |
|  | Listwa zasilająca | | | Liczba gniazd wyjściowych: 5 szt., długość przewodu zasilającego: 1,8 metra, napięcie znamionowe: 230 V AC, prąd znamionowy: 10 A, częstotliwość: 50 Hz, absorpcja energii: 150J, Maksymalny prąd impulsu: 6500 A, ,maksymalny czas reakcji: 25 ns, bezpiecznik nadprądowy: 2x10A/250V (topikowy), możliwość montażu na ścianie |
| Oprogramowanie | | | | |
|  | | Pakiet biurowy | Microsoft Office PL zawierający min.: Word - edytor tekstu, Excel - arkusz kalkulacyjny, PowerPoint - program do tworzenia prezentacji, Outlook - menedżer poczty elektronicznej oraz informacji, lub równoważny | |
|  | | Pakiet antywirusowy | Wersja kompatybilna z oferowanym systemem operacyjnym, zapewniająca dostęp do bazy sygnatur wirusów przez okres 2 lat (wymagania techniczne określone w pkt. 5.2) | |
|  | | System monitoringu | Wymagana jest dostawa oraz konfiguracja specjalizowanego oprogramowania (wraz z wszelkimi niezbędnymi licencjami) pełniącego funkcję systemu monitoringu budowanej infrastruktury sieciowej (zgodnie z wymaganiami określonymi w pkt. 4.7.4.1) | |
| Gwarancja | | | | |
|  | | Komputer  Monitor  Pozostały sprzęt | 3 lata w miejscu eksploatacji  Czas reakcji serwisu - do końca następnego dnia roboczego  Oferent musi posiadać autoryzacje producenta stacji – dokumenty potwierdzające załączyć do oferty  Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta – dokumenty potwierdzające załączyć do oferty.  Oświadczenie producenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem gwarancyjnym | |

4.7.4.1. Wymagania funkcjonalne systemu Monitoringu:

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 dostępności (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 i ich magazynowanie na serwerze pamięci masowej
* analiza zdarzeń SYSLOG z opisem znaczenia danego zdarzenia i sugestią rozwiązania danego problemu

Wymagania gwarancyjno serwisowe dla serwerów i urządzeń (wymienionych w pkt. 4.7 niniejszej specyfikacji)

* W celu zachowania pełnej kompatybilności i spójności rozwiązania, oraz uproszczenia zarządzania i administracji - wszystkie urządzenia (Cechy: 1, 2, 4) powinny pochodzić od tego samego producenta (całość dostarczanego sprzętu musi pochodzić z autoryzowanego kanału sprzedaży producenta na rynek polski)
* Całość dostarczanego sprzętu musi być nowa, nieużywana w wcześniejszych projektach.
* Wymagany jest 36 miesięczny serwis gwarancyjny na wszystkie urządzenia (Cechy: 1, 2, 3,4) świadczony bezpośrednio przez producenta w miejscu instalacji urządzeń z czasem reakcji NextBusinessDay od zgłoszenia awarii
* Oferent powinien posiadać status autoryzowanego partnera producenta oferowanego przez siebie sprzętu (Cechy: 1, 2, 4) – do oferty należy dołączyć stosowny certyfikat potwierdzający posiadanie takiego statusu.
* Wszystkie urządzenia (Cechy 1, 2, 3, 4,) powinny być objęte 36 miesięczną gwarancją producenta.

1. **Dostawa oraz instalacja sprzętu komputerowego do uczestników projektu**

Wykonawca jest zobowiązany do skalkulowania wszelkich kosztów związanych z dostawą oraz instalacją sprzętu komputerowego na miejscu (u Beneficjentów ostatecznych).

* 1. Zestaw Komputerowy – (40 szt.)

**Cecha 5**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Lp. | Nazwa atrybutu | | Wymagania minimalne | |
| Komputer stacjonarny przeznaczony do zapewnienia beneficjentom końcowym projektu dostępu do sieci Internet, dedykowany do obsługi aplikacji biurowych, grafiki prezentacyjnej, multimediów i nauczania na odległość | | | | |
|  | | Wydajność | | Procesor klasy x86, dedykowany do pracy w komputerach stacjonarnych uzyskujący przy pracy w nominalnych warunkach w teście Passmark CPU Mark wynik min. 2300 punktów (wynik zaproponowanego procesora musi znajdować sie na stronie <http://www.cpubenchmark.net> , zaś wydruk potwierdzenia dołączony do oferty) |
|  | | Pamięć | | min. 2GB pamięci operacyjnej DDR3 1333MHz z możliwością rozbudowy do 4GB  min. 250GB pamięci masowej SATAII 7200rpm |
|  | | Grafika | | Zintegrowana, z możliwością dynamicznego przydzielenia pamięci w obrębie pamięci systemowej do 512MB ze wsparciem dla DirectX 10, API i OpenGL 2.0 |
|  | | Napędy wbudowane | | Nagrywarka DVD +/-RW wraz z oprogramowaniem do nagrywania płyt |
|  | | Funkcjonalność BIOS | | - Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS)  - Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń  - Możliwość polegająca na kontrolowaniu urządzeń wykorzystujących magistralę komunikacyjną PCI, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych. Pod pojęciem kontroli Zamawiający rozumie funkcjonalność polegającą na blokowaniu/odblokowaniu slotów PCI.  - Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na poziomie systemu, administratora oraz dysku twardego oraz możliwość ustawienia następujących zależności pomiędzy nimi: brak możliwości zmiany hasła pozwalającego na uruchomienie systemu bez podania hasła administratora.  - Musi posiadać możliwość ustawienia zależności pomiędzy hasłem administratora a hasłem systemowy tak, aby nie było możliwe wprowadzenie zmian w BIOS wyłącznie po podaniu hasła systemowego. Funkcja ta ma wymuszać podanie hasła administratora przy próbie zmiany ustawień BIOS w sytuacji, gdy zostało podane hasło systemowe.  - Możliwość odczytania z BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych , informacji na temat: zainstalowanego procesora, pamięci operacyjnej RAM wraz z informacją o obsadzeniu slotów pamięci, obsadzeniu slotów PCI.  - Możliwość włączenia/wyłączenia zintegrowanej karty dźwiękowej, karty sieciowej, portu równoległego, portu szeregowego z poziomu BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.  - Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne.  - Możliwość wyłączania portów USB w tym: wszystkich portów, tylko portów znajdujących się na przodzie obudowy.  - Możliwość zmiany trybu pracy dysku twardego: na pracę zapewniającą największą wydajność, na pracę zmniejszającą poziom hałasu generowanego przez dysk twardy.  - Możliwość zablokowania zapisu na dyskietki |
|  | | Funkcjonalność obudowy | | * zasilacz o mocy min.255W * możliwość zastosowania zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki) * możliwość zamontowania urządzeń (1x 5,25” zewnętrzne, 1x 3,5” zewnętrzne, 1x 3,5” wewnętrzne). Wnęki pełnej wysokości, nie dopuszcza się napędów typu slim. * przystosowanie do pracy w pozycji pionowej i poziomej * konstrukcja pozwalająca na otwarcie obudowy oraz montaż/demontaż kart rozszerzeń i napędów bez konieczności użycia narzędzi, * wbudowany czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym producenta komputera; * wbudowany wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami; a w szczególności musi sygnalizować: * Przebieg procedury POST * Sum kontrolnych BIOSu * Awarii procesora lub pamięci podręcznej procesora * Uszkodzenia lub braku pamięci RAM, uszkodzenia złączy PCI, kontrolera Video, dysku twardego, płyty głównej, kontrolera USB |
|  | | Oprogramowanie | | Microsoft Windows 7 Home Premium PL 32-bit, zainstalowany system operacyjny niewymagający aktywacji za pomocą telefonu lub Internetu w firmie Microsoft. Dołączony nośnik z oprogramowaniem |
|  | | Certyfikaty i standardy | | Wymagane są dokumenty poświadczające:   * Certyfikat ISO 9001:2000 dla producenta sprzętu (do oferty należy załączyć kopie certyfikatu potwierdzającą spełnianie wymogu) * Certyfikat ISO 14001 dla producenta sprzętu (do oferty należy załączyć kopie certyfikatu potwierdzającą spełnianie wymogu) * Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z systemem operacyjnym Windows 7 (do oferty należy załączyć wydruk ze strony Microsoft) * Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie jałowym (IDLE) wynosząca maksymalnie 19dB (załączyć oświadczenie producenta) * Deklaracja CE (należy załączyć do oferty dokument potwierdzający spełnienie wymogu) * Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia wykonawcy wystawionego na podstawie dokumentacji producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram * Certyfikat EPEAT na poziomie GOLD   Wymagany wpis dotyczący oferowanego komputera w internetowym katalogu <http://www.epeat.net> - dopuszcza się wydruk ze strony internetowej |
|  | | Wsparcie techniczne producenta | | Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.  Dołączony nośnik ze sterownikami. |
|  | | Wymagania dodatkowe | | - Płyta główna zaprojektowana przez producenta jednostki centralnej komputera, wyposażona w min. 2 sloty PCI i 1 slot PCI-Express x16 (ze wsparciem dla PCIe x1, dopuszcza się złącza Low Profile), 2 złącza DIMM, kontroler SATA II (dla min. 3 urządzeń)  - Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, 4 kanałowa  - Karta sieciowa wbudowana: 10/100/1000Mbit/s, Ethernet RJ 45, PXE/RPL, ASF, WoL  - Wbudowane porty: 1 x LPT; 1 x RS232, 1 x VGA; min. 8 x USB w tym min. 2 z przodu obudowy; wymagana ilość portów nie może być uzyskana poprzez stosowanie przejściówek lub kart PCI  - Czytnik kart multimedialnych 8-in-1  - Klawiatura USB w układzie polski programisty, Mysz optyczna USB z sześcioma klawiszami oraz rolką (scroll) min 1000dpi |
| Monitor | | | | |
|  | | Typ ekranu | | Ekran ciekłokrystaliczny z aktywną matrycą TFT 18,5” |
|  | | Rozmiar plamki | | 0,300 mm |
|  | | Jasność | | 250 cd/m2 |
|  | | Kontrast | | 1000:1 |
|  | | Kąty widzenia (pion/poziom) | | 160/160 stopni |
|  | | Czas reakcji matrycy | | max 5ms |
|  | | Rozdzielczość maksymalna | | 1366 x 768 przy 60Hz |
|  | | Częstotliwość odświeżania poziomego | | 30 – 83 kHz |
|  | | Częstotliwość odświeżania pionowego | | 56 – 76 Hz |
|  | | Pochylenie monitora | | W zakresie od -4 do +21 stopni |
|  | | Powłoka powierzchni ekranu | | Antyodblaskowa |
|  | | Podświetlenie | | System podświetlenia 2 CCFL |
|  | | Bezpieczeństwo | | Możliwość zastosowania zabezpieczenia fizycznego w postaci linki metalowej |
|  | | Zużycie energii | | 19 W(typowe); 23 W(maksymalnie), |
|  | | Złącze | | 15-stykowe złącze D-Sub |
|  | | Certyfikaty i standardy | | Wymagane są dokumenty poświadczające:  - Energy Star, ISO 13406-2 lub ISO 9241, TCO 03  - Certyfikat ISO9001 oraz ISO14001 dla producenta sprzętu  - Deklaracja zgodności CE |
|  | | Inne | | Zdejmowana podstawa oraz otwory montażowe w obudowie VESA 100mm |
|  | | Głośniki | | Stereo, przystosowane do integracji z obudową monitora |
| Oprogramowanie | | | | |
|  | Pakiet biurowy | | Microsoft Office PL zawierający min.: Word - edytor tekstu, Excel - arkusz kalkulacyjny, PowerPoint - program do tworzenia prezentacji - wersja uprawniająca do przenoszenia licencji, lub równoważny | |
|  | Pakiet antywirusowy | | Wersja kompatybilna z oferowanym systemem operacyjnym, zapewniająca dostęp do bazy sygnatur wirusów przez okres 2 lat (wymagania techniczne określone w pkt. 5.2) | |
| Gwarancja | | | | |
|  | Komputer  Monitor | | 5 lat w miejscu eksploatacji  Czas reakcji serwisu - do końca następnego dnia roboczego  Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera oraz monitora – dokumenty potwierdzające załączyć do oferty.  Oświadczenie producentów komputera i monitora, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem gwarancyjnym. | |
|  | Pozostały sprzęt | | 3 lata w miejscu eksploatacji | |

* 1. Oprogramowanie antywirusowe oraz antyspyware, wraz z konsolą do zdalnej administracji

1. Pełne wsparcie dla systemu Windows NT 4.0 z sp6 /2000/XP/PC Tablet/Vista/Windows 7

2. Wsparcie dla Windows Security Center (Windows XP SP2).

3. Wsparcie dla 32- i 64-bitwej wersji systemu Windows.

4. Wersja programu dla stacji roboczych Windows dostępna zarówno języku polskim jak i angielskim.

5. Pomoc w programie (help) w języku polskim.

6. Dokumentacja do programu dostępna w języku polskim.

7. Skuteczność programu potwierdzona nagrodami VB100 i co najmniej dwie inne niezależne organizacje np. ICSA labs lub Check Mark.

Ochrona antywirusowa i antyspyware

8. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.

9. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.

10. Wbudowana technologia do ochrony przed rootkitami.

11. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

12. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.

13. System powinien 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.

14. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).

15. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.

16. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.

17. Możliwość skanowania dysków sieciowych i dysków przenośnych.

18. Skanowanie plików spakowanych i skompresowanych.

19. Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (w tym z uwzględnieniem plików bez rozszerzeń).

20. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.

21. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.

22. 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.

23. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego).

24. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird i Windows Live Mail

25. Skanowanie i oczyszczanie poczty przychodzącej POP3 "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).

26. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.

27. Możliwość definiowania różnych portów dla POP3, na których ma odbywać się skanowanie.

28. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.

29. Możliwość skanowania na żądanie lub według harmonogramu baz Outlook Express-a.

30. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.

31. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występujące w nawie strony.

32. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.

33. Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie.

34. 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.

35. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.

36. Aktualizacje modułów analizy heurystycznej.

37. 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 powinny być wysyłane automatycznie, oraz czy próbki zagrożeń powinny być wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.

38. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.

39. Wysyłanie zagrożeń do laboratorium powinno być możliwe z serwera zdalnego zarządzania i lokalnie z każdej stacji roboczej w przypadku komputerów mobilnych.

40. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń powinny być w pełni anonimowe.

41. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.

42. Możliwość automatycznego wysyłania powiadomienia o wykrytych zagrożeniach do dowolnej stacji roboczej w sieci lokalnej.

43. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e mail.

44. Interfejs programu powinien oferować funkcję pracy w trybie bez grafiki gdzie cały interfejs wyświetlany jest w formie formatek i tekstu.

45. Interfejs programu powinien mieć możliwość automatycznego aktywowania trybu bez grafiki w momencie, gdy użytkownik przełączy system Windows w tryb wysokiego kontrastu.

46. Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS i POP3S.

47. Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.

48. Administrator powinien mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.

49. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.

50. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program powinien pytać o hasło.

51. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji powinno być takie samo.

52. Program powinien być w pełni zgodny z technologią CISCO NAC.

53. Program powinien mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.

54. Program powinien 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, powinna także istnieć opcja dezaktywacji tego mechanizmu.

55. Po instalacji programu, użytkownik powinien 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.

56. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB powinien umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.

57. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB powinien pracować w trybie graficznym.

58. Program powinien umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: stacji dyskietek, napędów CD/DVD oraz portów USB.

59. Funkcja blokowania portów USB powinna umożliwiać administratorowi zdefiniowanie listy portów USB w komputerze, które nie będą blokowane (wyjątki).

60. W programie powinien być wyposażony w 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.

61. Funkcja generująca taki log powinna oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.

62. Program powinien 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.

63. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.

64. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej (program antywirusowy z wbudowanym serwerem HTTP).

65. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.

66. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja).

67. Do każdego zadania aktualizacji można przypisać dwa różne profile z innym ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja).

68. Możliwość przypisania 2 profili aktualizacyjnych z różnymi ustawieniami do jednego zadania aktualizacji. Przykładowo, domyślny profil aktualizuje z sieci lokalnej a w przypadku jego niedostępności wybierany jest profil rezerwowy pobierający aktualizację z Internetu.

69. Program wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

70. Praca programu musi być niezauważalna dla użytkownika.

71. Program powinien posiadać dwie wersje interfejsu (standardowy – z ukrytą częścią ustawień oraz zaawansowany – z widocznymi wszystkimi opcjami)

72. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania.

73. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

Konsola zdalnej administracji

1. Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych Windows.

2. Zdalna instalacja wszystkich wersji programów na stacjach roboczych NT 4.0 sp4/2000/XP Professional/PC Tablet/ Vista/Windows7.

3. Do instalacji zdalnej i zarządzania zdalnego nie jest wymagany dodatkowy agent. Na końcówkach zainstalowany jest sam program antywirusowy

4. Komunikacja miedzy serwerem a klientami może być zabezpieczona hasłem.

5. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware’ową zainstalowanymi na stacjach roboczych w sieci korporacyjnej z jednego serwera zarządzającego

6. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych z opcją wygenerowania raportu ze skanowania i przesłania do konsoli zarządzającej.

7. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie i skanerów rezydentnych).

8. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, adresów MAC, wersji systemu operacyjnego oraz domeny, do której dana stacja robocza należy.

9. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.

10. Możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych.

11. Możliwość tworzenia grup stacji roboczych i definiowania w ramach grupy wspólnych ustawień konfiguracyjnymi dla zarządzanych programów.

12. Możliwość importowania konfiguracji programu z wybranej stacji roboczej a następnie przesłanie (skopiowanie) jej na inną stację lub grupę stacji roboczych w sieci.

13. Możliwość zmiany konfiguracji na stacjach z centralnej konsoli zarządzającej lub lokalnie (lokalnie tylko jeżeli ustawienia programu nie są zabezpieczone hasłem lub użytkownik/administrator zna hasło zabezpieczające ustawienia konfiguracyjne).

14. Możliwość uruchomienia serwera zdalnej administracji na stacjach Windows NT 4.0 (Service Pack 6)/2000/XP/Vista/Windows 7 oraz na serwerach Windows NT 4.0 (Service Pack 6)//2000/2003/2008 – 32 i 64-bitowe systemy.

15. Możliwość uruchomienia centralnej konsoli zarządzającej na stacji roboczej Windows 2000/XP/Vista/Windows7, oraz na serwerach Windows 2000/2003/2008 - 32 i 64-bitowe systemy.

16. Możliwość wymuszenia konieczności uwierzytelniania stacji roboczych przed połączeniem się z serwerem zarządzającym. Uwierzytelnianie przy pomocy zdefiniowanego na serwerze hasła.

17. Do instalacji serwera centralnej administracji nie jest wymagane zainstalowanie żadnych dodatkowych baz typu MSDE lub MS SQL. Serwer centralnej administracji musi mieć własną wbudowaną bazę w pełni kompatybilną z formatem bazy danych programu Microsoft Access.

18. Serwer centralnej administracji powinien oferować administratorowi możliwość współpracy przynajmniej z trzema zewnętrznymi motorami baz danych w tym minimum z: Microsoft SQL Server, MySQL Server oraz Oracle.

19. Do instalacji serwera centralnej administracji nie jest wymagane zainstalowanie dodatkowych aplikacji takich jak Internet Information Service (IIS) czy Apache.

20. Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) w formacie HTML lub CSV.

21. Możliwość tworzenia hierarchicznej struktury serwerów zarządzających i replikowania informacji pomiędzy nimi w taki sposób, aby nadrzędny serwer miał wgląd w swoje stacje robocze i we wszystkie stacje robocze serwerów podrzędnych (struktura drzewiasta).

22. Serwer centralnej administracji powinien oferować funkcjonalność synchronizacji grup komputerów z drzewem Active Directory. Synchronizacja ta, powinna automatycznie umieszczać komputery należące do zadanych grup w AD do odpowiadających im grup w programie. Funkcjonalność ta nie powinna wymagać instalacji serwera centralnej administracji na komputerze pełniącym funkcję kontrolera domeny.

23. Serwer centralnej administracji powinien umożliwiać definiowanie różnych kryteriów wobec podłączonych do niego klientów (w tym minimum przynależność do grupy roboczej, przynależność do domeny, adres IP, adres sieci/podsieci, zakres adresów IP, nazwa hosta, przynależność do grupy, brak przynależności do grupy). Po spełnieniu zadanego kryterium lub kilku z nich stacja powinna otrzymać odpowiednią konfigurację.

24. Serwer centralnej administracji powinien być wyposażony w mechanizm informowania administratora o wykryciu nieprawidłowości w funkcjonowaniu oprogramowania zainstalowanego na klientach w tym przynajmniej informowaniu o: wygaśnięciu licencji na oprogramowanie, o tym że zdefiniowany procent z pośród wszystkich stacji podłączonych do serwera ma nieaktywną ochronę oraz że niektórzy z klientów podłączonych do serwera oczekują na ponowne uruchomienie po aktualizacji do nowej wersji oprogramowania.

25. Serwer centralnej administracji powinien być wyposażony w wygodny mechanizm zarządzania licencjami, który umożliwi sumowanie liczby licencji nabytych przez użytkownika. Dodatkowo serwer powinien informować o tym, ilu stanowiskową licencję posiada użytkownik i stale nadzorować ile licencji spośród puli nie zostało jeszcze wykorzystanych.

26. W sytuacji, gdy użytkownik wykorzysta wszystkie licencje, które posiada po zakupie oprogramowania, administrator po zalogowaniu się do serwera poprzez konsolę administracyjną powinien zostać poinformowany o tym fakcie za pomocą okna informacyjnego.

27. Możliwość tworzenia repozytorium aktualizacji na serwerze centralnego zarządzania i udostępniania go przez wbudowany serwer http.

28. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

29. Dostęp do kwarantanny klienta z poziomu systemu zdalnego zarządzania.

30. Możliwość przywrócenia lub pobrania zainfekowanego pliku ze stacji klienckiej przy wykorzystaniu zdalnej administracji

31. Administrator powinien mieć możliwość przywrócenia i wyłączenia ze skanowania pliku pobranego z kwarantanny stacji klienckiej

32. Podczas przywracania pliku, administrator powinien mieć możliwość zdefiniowania kryteriów dla plików które zostaną przywrócone w tym minimum: zakres czasu z dokładnością co do minuty kiedy wykryto daną infekcję, nazwa danego zagrożenia, dokładna nazwa wykrytego obiektu oraz zakres minimalnej i maksymalnej wielkości pliku z dokładnością do jednego bajta.

33. Możliwość utworzenia grup, do których przynależność jest aplikowana dynamicznie na podstawie zmieniających się parametrów klientów w tym minimum w oparciu o: wersję bazy sygnatur wirusów, maskę wersji bazy sygnatur wirusów, nazwę zainstalowanej aplikacji, dokładną wersję zainstalowanej aplikacji, przynależność do domeny lub grupy roboczej, przynależność do serwera zdalnego zarządzania, przynależności lub jej braku do grup statycznych, nazwę komputera lub jej maskę, adres IP, zakres adresów IP, przypisaną politykę, czas ostatniego połączenia z systemem centralnej administracji, oczekiwania na restart, ostatnie zdarzenie związane z wirusem, ostatnie zdarzenie związane z usługą programu lub jego procesem, ostatnie zdarzenie związane ze skanowaniem na żądanie oraz z nieudanym leczeniem podczas takiego skanowania, maską wersji systemu operacyjnego oraz flagą klienta mobilnego.

34. Podczas tworzenia grup dynamicznych, parametry dla klientów można dowolnie łączyć oraz dokonywać wykluczeń pomiędzy nimi.

35. Utworzone grupy dynamiczne mogą współpracować z grupami statycznymi.

1. **Usługi serwisowania i administrowania siecią szerokopasmową oraz serwis i utrzymanie sprzętu komputerowego przez okres 36 miesięcy**
   1. Serwis i utrzymanie infrastruktury sieci szerokopasmowej

Wykonawca zobowiązuje się do utrzymywania, serwisowania oraz administracji infrastrukturą sieci szerokopasmowej w następującym zakresie:

-bieżące monitorowanie infrastruktury i wykrywanie awarii

-bieżące usuwanie awarii w ciągu maksymalnie 8 godzin – dotyczy warstwy szkieletowej sieci (radiolinie cyfrowe, stacje bazowe WiMAX, urządzenia aktywne stanowiące wyposażenie Głównego Węzła Dystrybucyjnego oraz Centrum Zarządzania siecią)

- bieżące usuwanie awarii w ciągu maksymalnie 48 godzin – pozostałe elementy infrastruktury

- uruchomienia telefonicznego centrum serwisowego dla uczestników projektu, działającego w godzinach od 8.00 – do 20.00 w dni robocze

- sporządzanie okresowych raportów obciążenia infrastruktury sieciowej, (radiolinii, stacji bazowych, punktów dostępowych WiFi oraz innych urządzeń)

- prowadzenie elektronicznej ewidencji zgłoszeń serwisowych

* 1. Serwis i utrzymywanie sprzętu komputerowego w gospodarstwach domowych (40 zestawów komputerowych z dostępem do Internetu)

Wykonawca zobowiązany jest do dostarczenia i instalacji 40 szt. sprzętu komputerowego ( zestawów komputerowych oraz urządzeń umożliwiających korzystanie z usługi dostępu do Internetu) w lokalizacjach (gospodarstwach domowych) określonych przez zamawiającego.

Wykonawca zobowiązany do świadczenia usługi utrzymywania, serwisowania i konserwacji sprzętu komputerowego (w tym również usług dostępu do Internetu) w gospodarstwach domowych, a w szczególności:

- świadczenia usług serwisu sprzętu komputerowego w miejscu instalacji

- świadczenia usług wsparcia technicznego poprzez określenie wydzielonego nr telefonu serwisowego przeznaczonego dla mieszkańców objętych projektem (tzw. grupy docelowej)

- podjęcia działań serwisowych w ciągu maksymalnie 8 godzin od momentu zgłoszenia awarii

- usunięcia usterki (naprawy) w ciągu najpóźniej 2 dni roboczych od momentu zgłoszenia awarii

1. **Zapewnienie usługi dostępu do Internetu dla 100 gospodarstw domowych oraz 14 jednostek podległych przez okres 36 miesięcy.**
   1. Dostawa, montaż i konfiguracja urządzeń dostępowych dla 100 gospodarstw domowych

Wymagana jest dostawa urządzeń, (lub zestawu urządzeń) zapewniających podłączenie komputera do Internetu dla 100 gospodarstw domowych (Beneficjentów końcowych projektu) , ich instalacja oraz konfiguracja a także uruchomienie.

Dokładne dane lokalizacji montowanych urządzeń dostępowych zostaną wskazane przez Zamawiającego w załączniku do umowy.

Wymagania ogólne

1. Wykonawca dostarczy wszelkie urządzenia potrzebne do skonfigurowania połączeń: urządzenia dostępowe, okablowanie oraz jeśli to będzie wymagane maszty i elementy mocowania anten
2. urządzenia dostępowe muszą posiadać interfejs LAN (Ethernet 10/100, RJ-45), tak aby była możliwość podłączenia komputera bez ingerencji w komputer oraz bez konieczności montażu przez Zamawiającego dodatkowego okablowania
3. Zamawiający wyklucza rozwiązania oparte na kartach rozszerzeń montowanych wewnątrz obudowy komputera
4. Wykonawca będzie zobowiązany do konfiguracji, utrzymania i serwisowania dostarczonych i zainstalowanych urządzeń przez okres 36 miesięcy, a w szczególności:

- podjęcia działań serwisowych w ciągu maksymalnie 24 godzin od momentu zgłoszenia awarii

- usunięcia usterki (naprawy) w ciągu najpóźniej 2 dni roboczych od momentu zgłoszenia awarii

- 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

1. Wszystkie urządzenia powinny posiadać 36 miesięczną gwarancję

Minimalne wymagania funkcjonalne i techniczne

* Urządzenie przeznaczone do zastosowań zewnętrznych (wyposażone w zestaw montażowy)
* Temperatura pracy: od -30C do 80C
* Wilgotność pracy: 5 to 95%
* Urządzenie pracujące w standardzie IEEE 802.11n 2x2 MIMO
* Urządzenie zintegrowane z dwu-polaryzacyjną anteną o zysku minimum 14 dBi
* Moduł radiowy o mocy max 23 dBm i czułości -96 dBm
* Procesor: Atheros MIPS 24KC, 400MHz
* Pamięć: 32MB SDRAM, 8MB Flash
* Wyposażone w interfejs sieciowy 2x10/100 BASE-TX (Cat. 5, RJ-45)
* Pobór mocy: max 10 Wat
* Zasilanie: 15V POE Adapter (POE-24)
* Metoda zasilania: Pasywny POE
* Waga: max. 1 kg
* Regulacje prawne: Potwierdzenia FCC Part 15.247, IC RS210, CE, RoHS
  1. Usługa dostępu do Internetu

Zamawiający wymaga świadczenia usług dostępu do Internetu dla 100 gospodarstw domowych oraz 14 jednostek podległych Gminy Bojanów, przez okres 36 miesięcy

Usługa świadczona będzie w postaci łącza internetowego klasy operatorskiej zestawionego w jednym z Węzłów Rdzeniowych sieci, lub w lokalizacji Centrum Zarządzania siecią o następujących parametrach:

- łącze powinno być zestawione w technologii światłowodowej lub za pomocą radiolinii cyfrowej pracującej w licencjonowanym paśmie radiowym, Zamawiający nie dopuszcza możliwości wykorzystania radiolinii wykorzystujących nielicencjonowane pasmo radiowe.

- przepustowość łącza dostępu do Internetu nie mniejsza niż 40 Mb/s FDD

- brak limitu transferu danych

- brak limitów i ograniczeń czasowych korzystania z usługi

- zapewnienie puli zewnętrznych adresów IP w minimalnej ilości 256 (w ramach jednej klasy C)

Ponadto wykonawca w ramach usługi zapewni wszelkie dodatkowe urządzenia, niezbędne do uruchomienia i świadczenia usługi (router, modemy, media konwertery itp.)

1. **Szkolenia z zakresu obsługi komputera (systemu operacyjnego, pakietu biurowego oraz Internetu).**

Wymagania w zakresie szkoleń:

- W celu zapewnienia wysokiej jakości poziomu szkolenia, Wykonawca powinien dysponować min. 2 wykwalifikowanymi osobami, posiadającymi uprawienia na poziomie trenera/egzaminatora ECDL

- Wykonawca zapewni sale szkoleniowe przystosowane do prowadzenia zajęć

dydaktycznych wyposażone w niezbędne pomoce dydaktyczne, w co najmniej projektor multimedialny, ekran, tablice, plansze itp., na minimum 15 miejsc szkoleniowych, z dostępem do Internetu,

- Wykonawca zapewni wystarczającą liczbę własnych licencji na oprogramowanie wykorzystywane przy realizacji szkoleń

- Prowadzenie list obecności na szkoleniach

- Zapewnienie materiałów szkoleniowych

- Program szkolenia powinien obejmować następujące zagadnienia:

1. Podstawy obsługi komputera i systemu Windows

a. Podstawowe pojęcia związane z budową komputera oraz sieciami

komputerowymi

b. Podstawowe zasady pracy z komputerem przenośnym (budowa, zasady

obsługi, obsługa urządzeń peryferyjnych, klawiatura)

c. Podstawowe informacje o systemie operacyjnym

d. Uruchamianie i zamykanie systemu

e. Obsługa aplikacji (uruchamianie, okno aplikacji, menu, zamykanie)

f. Foldery, pliki (tworzenie, zapisywanie, wyszukiwanie)

2. Pakiet biurowy Office

a. Ogólna prezentacja

b. Edytor tekstu

i. Okno programu

ii. Podstawowe zasady tworzenia dokumentów tekstowych

iii. Tworzenie i zapisywanie nowych dokumentów

iv. Formatowanie tekstów (czcionka, efekty, rozmiar)

v. Zastosowanie szablonów dokumentów

c. Arkusz kalkulacyjny

i. Zastosowania programu

ii. Okno programu

iii. Tworzenie prostych tabel

iv. Formatowanie tabel

v. Zastosowanie szablonów tabel

d. Kalendarze

i. Zastosowania programu

ii. Okno programu

iii. Tworzenie kalendarzy i harmonogramów oraz zadań

3. Internet i poczta elektroniczna

a. Ogólne zasady korzystania z Internetu

b. Przeglądarka internetowa

i. Okno programu

ii. Adres internetowy

iii. Otwieranie i przeglądanie stron internetowych

iv. Ulubione – zapisywanie najczęściej otwieranych stron internetowych

c. Poczta elektroniczna

i. Klient pocztowy (okno programu)

ii. Adres pocztowy

iii. Wysyłanie, odbieranie, usuwanie poczty elektronicznej

iv. Książka adresowa

4. Bezpieczeństwo systemów informatycznych

a. Ogólne zasady bezpieczeństwa związane z obsługą komputera i dostępem do Internetu

b. Programy antywirusowe

Przed rozpoczęciem szkoleń, wykonawca przedstawi zamawiającemu szczegółowy program szkoleń do akceptacji.

1. **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 obiektuoraz 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.

**Uwaga!**

**Zaleca się dokonanie wizji lokalnej dla w/w zakresu robót przed złożeniem oferty, oraz szczegółowe zapoznanie się z dokumentacją przetargową.**

* 1. Szkolenia dla administratorów sieci

W ramach dostawy wymagane jest przeprowadzenie szkolenia dla wyznaczonych pracowników Zamawiającego w zakresie:

* Konfiguracji i zarządzania radioliniami cyfrowymi
* Podstawowej konfiguracji i zarządzania urządzeniami aktywnymi sieci
* Administracja i zarządzanie systemem WiMAX
* Administracja i zarządzanie bezprzewodowa siecią WLAN ( kontroler sieci bezprzewodowej)
* Zarządzania systemem LMS
* Polityki autentykacji i autoryzacji użytkowników sieci
* Wykonywania kopii bezpieczeństwa, plików konfiguracyjnych itp.
  1. Dokumenty odbioru końcowego
* Dzienniki budowy.
* 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,
* Odpowiednie atesty i certyfikaty
* Instrukcje obsługi, dokumentacje i inne dokumenty dostarczane wraz ze sprzętem, przez producenta
* Raport z przeprowadzonego szkolenia dla administratorów sieci

1. **CZĘŚĆ INFORMACYJNA PROGRAMU**
   1. Akty prawne i rozporządzenia:
   2. „Ustawa Prawo telekomunikacyjne z dnia 16 lipca 2004 roku”.
   3. „Ustawa o świadczeniu usług droga elektroniczna z dnia 18 lipca 2002 roku”
   4. „Ustawa o dostępie warunkowym”
   5. „Ustawie z dnia 18 września 2001 r. o podpisie elektronicznym”.
   6. „Ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne z dnia 17 lutego 2005 roku”.
   7. Prawo Ochrony Środowiska z dnia 27 kwietnia 2001r., w zakresie zasad ochrony środowiska oraz warunków korzystania z jego zasobów
   8. Rozporządzenie Rady Ministrów z dnia 21 sierpnia 2007 ( Dz. U. 2007 nr 158 poz. 1105)
   9. 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.)
   10. Rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 roku w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych,
   11. Rozporządzenie Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych
   12. Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych
   13. Uchwała Sejmu Rzeczypospolitej Polskiej z dnia 14 lipca 2000 r. w sprawie budowania podstaw społeczeństwa informacyjnego w Polsce.
   14. Ramy prawne Komisji Europejskiej w sektorze komunikacji elektronicznej
   15. 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.);
   16. 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.);
   17. 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.);
   18. 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.) ;
   19. 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.);
   20. 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.);
   21. Rozporządzenie (EC) 2887/2000 o niezależnym dostępie do pętli lokalnych
   22. Przy projektowaniu i budowie sieci radiowej należy wziąć pod uwagę następujące normy i rekomendacje komitetu ITU:
   23. Recommendation ITU-R 838, Specific Attenuation Model For Rain For Use In Prediction Methods
   24. Rekomendacja (zalecenie) ITU-R P.838-3: „Ścisły (specyficzny) model do zastosowania w metodach przewidywania tłumienia przez deszcz”
   25. Recommendation ITU-R P.676-3, Attenuation By Atmospheric Gases - Rekomendacja (zalecenie)

ITU-R P676.3: „Tłumienie przez gazy atmosferyczne”

* 1. 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”

* 1. 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”