

PROGRAM FUNKCJONALNO – UŻYTKOWY

w zakresie realizacji zadań inwestycyjnych
w ramach projektu pn.

„Przeciwdziałanie wykluczeniu cyfrowemu w Gminie Poraj”

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 13100-5 (komputery osobiste)
727 20000-3 (usługi w zakresie rozległej sieci komputerowej)
726 11000-6 (usługi w zakresie wsparcia technicznego)
442 122 63-0 Maszty kratowe
452 000 00-7 Roboty budowlane
453 000 00-0 Roboty instalacyjne w budynkach
805 000 00-9 (usługi szkoleniowe)

ZAMAWIAJĄCY:

Gmina Poraj
ul. Jasna 21
42-360 Poraj

Zawartość:

- I. Część opisowa programu
- II. Ogólne wymagania zamawiającego
- III. Aktualne uwarunkowania przedmiotu zamówienia
- IV. Ogólne właściwości funkcjonalno-użytkowe
- V. Szczegółowe właściwości i wymagania funkcjonalno-użytkowe
 1. W zakresie przygotowania dokumentacji projektowej, harmonogramu prac oraz pozostałej niezbędnej dokumentacji
 2. W zakresie budowy masztów antenowych oraz konstrukcji wsporczych pod anteny (elementy pasywne)
 3. W zakresie budowy sieci szkieletowej i połączeń dystrybucyjnych
 4. W zakresie budowy sieci dostępowej
 5. W zakresie budowy Głównego Węzła Dystrybucyjnego i Centrum Zarządzania siecią Gminy
 6. W zakresie dostawy i instalacji sprzętu komputerowego i oprogramowania
 7. W zakresie usługi administrowania i serwisowania systemu (sprzętu komputerowego oraz sieci szerokopasmowej)
 8. W zakresie zapewnienia usługi dostępu do Internetu dla Beneficjentów ostatecznych
 9. W zakresie organizacji szkoleń z podstaw obsługi komputera, pakietu biurowego, oraz obsługi Internetu
- VI. Ogólne warunki wykonania i odbioru robót
- VII. Część informacyjna programu

I. CZĘŚĆ OPISOWA PROGRAMU

Przedmiotem zamówienia jest kompleksowa realizacja zadania pn. „Przeciwdziałanie wykluczeniu cyfrowemu w Gminie Poraj” Szczegółowy zakres projektu składa się następujących zadań:

- 1. Przygotowania dokumentacji projektowej, harmonogramu prac oraz innej niezbędnej dokumentacji**
 - Opracowanie projektów budowlanych w zakresie budowy wież i/lub masztów antenowych (wraz z branżami), oraz niezbędną dokumentację związaną z uzyskaniem pozwolenia na budowę (jeśli będzie wymagane)
 - Wykonanie planowania radiowego
 - Opracowanie projektu wykonawczego budowy sieci szerokopasmowej
 - Opracowanie szczegółowego harmonogramu prac związanych robotami budowlanymi
- 2. Budowy wież i/lub masztów antenowych oraz konstrukcji wsporczych pod anteny**
 - Budowa wież i/lub masztów antenowych, ew. konstrukcji wsporczych
 - Instalacja szaf zewnętrznych lub wewnętrznych, w zależności od potrzeb oraz wykonanie instalacji teletechnicznych pod potrzeby instalacji infrastruktury
- 3. Budowy sieci szkieletowej oraz dystrybucyjnej**
 - Dostawa, instalacja oraz konfiguracja radiolinii cyfrowych
 - Dostawa, instalacja oraz konfiguracja połączeń dystrybucyjnych punkt-punkt
- 4. Budowy sieci dostępowej (Węzłów Dostępowych oraz instalacja terminali odbiorczych)**
 - Dostawa, instalacja i konfiguracja elementów oraz urządzeń stanowiących wyposażenie Węzłów Dostępowych
 - Dostawa, instalacja i konfiguracja przełączników sieciowych oraz UPSów
 - Montaż szaf, uchwytów antenowych oraz przygotowanie infrastruktury kablowej w obiektach Węzłów Dostępowych
 - Dostawa i instalacja i konfiguracja urządzeń odbiorczych dla Beneficjentów końcowych
- 5. Wyposażenia Głównego Węzła Dystrybucyjnego i Centrum Zarządzania siecią szerokopasmową.**
 - Adaptacja pomieszczenia przeznaczonego na Centrum Zarządzania
 - Dostawa, instalacja oraz konfiguracja urządzeń aktywnych 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)
- 6. Dostawa, instalacja sprzętu komputerowego i oprogramowania oraz jego modernizacja**
 - Dostawa 200szt. zestawów komputerowych wraz z oprogramowaniem dla gospodarstw domowych
 - Dostawa 66szt. komputerów wraz z oprogramowaniem dla jednostek podległych
- 7. Usługi administrowania i serwisowania systemu (sieci szerokopasmowej oraz sprzętu komputerowego), w tym kontrola ewentualnych nadużyć w okresie realizacji projektu (Operator Infrastruktury)**
 - Serwis i utrzymywanie sprzętu komputerowego w Jednostkach Podległych w ramach zadań koordynacyjnych
 - Serwis i utrzymywanie sprzętu komputerowego w gospodarstwach domowych
 - Serwis i utrzymanie infrastruktury sieci szerokopasmowej

**8. Zapewnienie usługi dostępu do Internetu dla gospodarstw domowych oraz Jednostkach Podległych przez okres realizacji projektu.
(Operator Infrastruktury)**

- Świadczenie usług dostępu do Internetu dla 200 gospodarstw domowych (BO) przez okres realizacji projektu
- Świadczenie usług dostępu do Internetu dla 14 Jednostek Podległych przez okres realizacji projektu

9. Szkolenia z podstaw obsługi komputera (systemu operacyjnego, pakietu biurowego oraz Internetu).

- przeprowadzenie szkoleń z podstaw obsługi komputera i Internetu dla 200 BO

Niniejszy program ma na celu umożliwienie dokonania wyboru najkorzystniejszej oferty na opracowanie dokumentacji projektowej oraz budowy infrastruktury sieci szerokopasmowej Gminy Poraj, 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

II. OGÓLNE WYMAGANIA ZAMAWIAJĄCEGO

Program funkcjonalno-użytkowy określa wymagania dotyczące zaprojektowania, realizacji i przekazania w użytkowanie wszystkich elementów opisywanego systemu. Wykonawca podejmujący się realizacji przedmiotu zamówienia zobowiązany jest po podpisaniu umowy 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: 2Mb/s
- Szybkość łącza Internetowego od użytkownika indywidualnego min: 512kbps
- 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)

2. Ogólne wymagania w zakresie technologii sieci bezprzewodowej

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

- Warstwa szkieletowa sieci powinna być wykonana w oparciu o radiolinie cyfrowe działające na licencjonowanych pasmach radiowych a połączenia dystrybucyjne punkt-punkt w oparciu o nielicencjonowane pasmo radiowe 5GHz
- Sieć w warstwie dostępowej powinna być oparta o technologię 802.11 a/b/g/n (obsługa MIMO) i działać na uwolnionych przez Urząd Komunikacji Elektronicznej częstotliwościach 2,4 Ghz oraz 5,47 – 5,725 GHz, z zachowaniem obowiązujących przepisów w tym zakresie, w szczególności maksymalnej mocy e.i.r.p.
- Wymaga się aby pojedyncze urządzenie punktu dostępowego (AP) posiadało 2 interfejsy radiowe tzw. Dual Band, każdy na inne pasmo uwolnione i bezpłatne w użytkowaniu
- węzły dostępowe winny być zainstalowane 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
- W projekcie założono, że we wskazanym przez Zamawiającego, lokalu użytkownika końcowego będzie instalowany radiowy terminal klienta typu zewnętrznego, który będzie bezpośrednio podłączony do zestawu komputerowego
- naziemna sieć bezprzewodowa powinna być zarządzana z Centrum Zarządzania, zlokalizowanego w budynku Urzędu Gminy Poraj i powinna zapewniać:
 - o zarządzanie użytkownikami i usługami sieci
 - o zarządzanie uszkodzeniami
 - o zarządzanie konfiguracją
 - o zarządzanie wydajnością
 - o zarządzanie bezpieczeństwem
 - o monitoring sieci
 - o autentykację użytkowników
 - o logowanie zdarzeń

W przypadku braku możliwości dostarczenia usługi dostępu do Internetu za pomocą budowanej przez Wykonawcę sieci bezprzewodowej (naziemnej) lub dostarczenie takie byłoby nie efektywne ekonomicznie lub technologicznie niemożliwe , dopuszczalne jest wykorzystanie w uzasadnionych przypadkach innych technologii, w tym satelitarnego dostępu do szerokopasmowego Internetu VSAT lub dostępu w standardzie GSM/CDMA/LTE, pod warunkiem zapewnienia obydwu kanałów (odbieranie i wysyłanie). Każdy taki przypadek musi być wcześniej uzgodniony z Zamawiającym.

W jednostkach podległych gminy, zamawiający oczekuje podłączenia jednego łącza internetowego dla całego obiektu, które zapewni dostęp do Internetu dla wszystkich dostarczonych do danej Jednostki zestawów komputerowych.

3. Ogólne wymagania obsługi gwarancyjno-serwisowej

- Wszystkie elementy wchodzące w skład przedmiotu zamówienia powinny być objęte 36 miesięczną gwarancją (o ile szczegółowe zapisy PFU nie stanowią inaczej)
- W okresie gwarancji Wykonawca zobowiązany jest zapewnić Zamawiającemu:
 - usuwanie wszelkich wad i nieprawidłowości powstałych na skutek standardowej i zgodnej z przeznaczeniem eksploatacji przedmiotu zamówienia
 - przyjmowanie zgłoszeń serwisowych w godzinach 8.00-20.00 (faks lub e-mail)
 - dostęp do wsparcia technicznego wraz z prawem do aktualizacji oprogramowania systemowego (w szczególności urządzeń sieciowych)
- Zamawiający oczekuje, że sprzęt dostarczony w ramach realizacji umowy będzie sprzętem nowym, nie używanym (dostarczanym) wcześniej w innych projektach.
- Jeżeli w trakcie trwania gwarancji, istnieje konieczność wykonywania płatnych okresowych przeglądów gwarancyjnych, wówczas przeglądy te będą wykonywane na koszt

Wykonawcy.

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

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

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

III. AKTUALNE UWARUNKOWANIA PRZEDMIOTU ZAMÓWIENIA

W ramach realizowanego projektu, planowana jest budowa infrastruktury teletransmisyjnej i teletechnicznej która zostanie zlokalizowana na działkach/objektach/budynkach należących do Gminy Poraj. Ze względu jednak na ukształtowanie i topografię terenu, dopuszcza się wykorzystanie budynków/objektów nie należących do Gminy. Jednak w pierwszej kolejności należy projektować lokalizację infrastruktury na obiektach należących do Gminy Poraj, a dopiero w następnej kolejności (po wcześniejszym uzgodnieniu z Zamawiającym) na ew. nieruchomościach prywatnych. Uzyskanie wszelkich zgód i pozwoleń związanych z lokalizacją infrastruktury na obiektach/budynkach właścicieli prywatnych, leży po stronie Wykonawcy.

Ponadto Wykonawca przedmiotu zamówienia dokona wszelkich niezbędnych uzgodnień administracyjnych, prawnych i projektowych wynikających z pozyskania obiektów celem lokalizacji węzłów sieci oraz przygotowania dokumentacji technicznej dla budowy sieci bezprzewodowej na terenie Gminy Poraj.

Wykonawca dokona wszelkich niezbędnych uzgodnień dodatkowych wynikających z wewnętrznych przepisów wprowadzonych przez właścicieli (zarządców) obiektów, na których będą prowadzone prace.

IV. OGÓLNE WŁAŚCIWOŚCI FUNKCJONALNO-UŻYTKOWE

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

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 dostępową (bezprowodowe 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 w Poraju oraz co najmniej 4 Węzły Rdzeniowe zlokalizowane na terenie Gminy Poraj.

W ramach połączeń szkieletowych, lokalizacje WR i GWD zostaną połączone radioliniami cyfrowymi klasy operatorskiej o przepustowości min. 100 Mb/s FDD. Zadaniem warstwy rdzenia sieci jest zapewnienie wysokiej wydajności transmisyjnej (min. 100 Mb/s FDD) i dostępności połączeń szkieletowych dla warstwy dystrybucyjnej i dostępowej sieci.

Warstwa dystrybucyjna

Warstwa dystrybucyjna sieci zostanie zbudowana w oparciu o połączenia radiowe punkt-punkt pracujące w oparciu o pasmo radiowe 5 GHz, zgodne ze standardem 802.11an (MIMO). Zadaniem tej warstwy jest dostarczanie wysokiej jakości usług transmisji danych oraz dostępu do Internetu.

W ramach projektu planowane jest podłączenie wszystkich jednostek podległych Gminy Poraj objętych projektem 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 z wykorzystaniem technik zwielokrotnienia torów radiowych MIMO.

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/n)
 - stosują modulację szerokopasmową,
 - moc wypromieniowywana EIRP jest mniejsza lub różna 100mW
- b) w paśmie 5470 ÷ 5725 MHz - (standard 802.11a/n)
 - 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.

Zamawiający określił następujące ogólne wymagania funkcjonalno-użytkowe:

- W jednym, wskazanym przez zamawiającego, lokalu użytkownika będzie instalowany jeden zestaw komputerowy wraz dostępem do Internetu
- We wskazanych jednostkach podległych będzie instalowana sieć LAN łącząca zestawy komputerowe z drukarką oraz urządzeniem odbiorczym/modemem w budynku. Ilość zestawów komputerowych podłączanych w poszczególnych lokalizacjach wskaże zamawiający.
- Okablowanie strukturalne (LAN) powinno być wykonane w oparciu o elementy kategorii 5.e
- System powinien umożliwiać dostęp wyłącznie autoryzowanym użytkownikom i stacjom roboczym
- System powinien monitorować zamawiającemu próbę podłączenia nieautoryzowanej jednostki lub udostępnienie Internetu poza lokal
- Urządzenia składowe muszą charakteryzować się trwałością funkcjonowania i zapewnić konstrukcyjnie min. 6 letni okres eksploatacji

- Sprzęt oraz zastosowana technologia ma spełniać nowoczesne standardy dla tego typu urządzeń, zarówno co do ich specyfikacji technicznych elementów elektronicznych, teleinformatycznych oraz mechanicznych - minimalne wymagania w tym zakresie zostały określone w dalszej części dokumentu
- System powinien zapewnić skalowalność, w przypadku rozszerzenia projektu o kolejnych beneficjentów

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

V. SZCZEGÓŁOWE WŁAŚCIWOŚCI I WYMAGANIA FUNKCJONALNO-UŻYTKOWE

1. Przygotowanie dokumentacji projektowej, harmonogramu prac oraz innej niezbędnej dokumentacji

Wykonawca zobowiązany jest do opracowania projektu sieci radiowej wraz z niezbędną dokumentacją budowlaną (jeśli będzie wymagana) oraz wykonawczą obejmującą teren Gminy Poraj (miejscowości objęte projektem) i powinna zawierać:

- projekty budowlane i projekty wykonawcze wież i/lub masztów antenowych – kompletne (wraz z branżami w przypadku konieczności uzyskania pozwolenia na budowę)
- planowanie radiowe zawierające wizualizację symulowanego pokrycia sygnałem radiowym:

- obejmujące swoim zakresem analizę dostarczanych systemów punkt-punkt oraz systemów punkt-wielopunkt
- zrealizowane w oparciu o mapy cyfrowe terenu (tzw. DTM)
- zrealizowane z wykorzystaniem rastrowych map wykorzystania (klas) terenu (tzw. landuse)
- zrealizowane z wykorzystaniem dodatkowej warstwy zabudowy (mapy wektorowe budynków z ich wysokością)

- 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 itp.) jak również mechanizmów kształtowania usług oraz zarządzania użytkownikami sieci.
- projekt implementacji mechanizmów bezpieczeństwa sieci
- monitorowania oraz logowania zdarzeń sieciowych.

Dokumentacja projektowa winna być kompletna z punktu widzenia celu, któremu ma służyć oraz spełniać wymogi określone przepisami:

- Ustawa z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych (Dz.U. z 2010 r. Nr 106 poz. 675 z późn. zm)
- 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 zachowania w/w przepisów i norm, oraz ew. innych aktów prawnych, 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 musi być wewnętrznie spójna i skorygowana we wszystkich branżach i zadaniach wyżej opisanych. Musi zawierać optymalne rozwiązania funkcjonalne, techniczne, konstrukcyjne, materiałowe i kosztowe. Wykonawca dokumentacji projektowej musi uzyskać, własnym staraniem i na własny koszt, wszystkie wymagane przepisami opinie i uzgodnienia.

2. Budowa wież i/lub masztów antenowych oraz konstrukcji wsporczych pod anteny

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

2.1 Budowa wież i/lub masztów antenowych, oraz konstrukcji wsporczych na potrzeby lokalizacji infrastruktury teletransmisyjnej –(min. 10kpl)

Projekt zakłada, budowę wież i/lub masztów antenowych na działkach którymi dysponuje Gmina Poraj oraz masztów o lekkiej konstrukcji, które będą instalowane na istniejących obiektach (budynekach) jednostek podległych Gminy. Zamawiający na prośbę wykonawcy udostępni pełną listę wszystkich jednostek podległych oraz wypis z rejestru gruntów. W przypadku braku możliwości lokalizacji infrastruktury na działkach, obiektach czy budynekach Gminy Poraj, dopuszcza się możliwość wykorzystania obiektów i budynków prywatnych po wcześniejszym uzgodnieniu z Zamawiającym. Wówczas uzyskanie ew. zgód właścicieli budynków prywatnych oraz ew. koszty z tym związane leżą po stronie Wykonawcy.

W związku z tym, że elementy konstrukcyjne oraz infrastruktura teletechniczna, jest budowana do celów instalacji urządzeń teletransmisyjnych (stacji bazowych, radiolinii, bezprzewodowych punktów dostępu) – ich dokładna lokalizacja powinna być wyznaczona na podstawie przeprowadzonego wcześniej przez Wykonawcę planowania radiowego.

W związku z planowaną budową min 4 Węzłów Rdzeniowych (WR), oraz min. 6 Węzłów Dystrybucyjnych (WD), wymagana jest budowa min. 10 szt. infrastruktury w postaci wież, masztów lub innych konstrukcji na potrzeby instalacji anten i urządzeń teletransmisyjnych stanowiących wyposażenie Węzłów sieci.

Wieże antenowe

- dopuszcza się budowę wież o konstrukcji stalowej kratownicowej lub strunobetonowych, wyposażonych w szynodrabinę z zabezpieczeniem przed upadkiem. Wieże powinny być posadowione na fundamencie osadzonym w gruncie. Wysokość wież powinna być określona na podstawie planowania radiowego oraz analizy ukształtowania terenu.

Maszty antenowe

- dopuszcza się budowę masztów antenowych o konstrukcji kratownicowej stalowych lub aluminiowych (w przypadku montażu na istniejących obiektach budowlanych). Maszty antenowe mogą być posadowione na fundamencie osadzonym w gruncie lub instalowane na istniejących budynkach . Wysokość masztów powinna być dobrana odpowiednio do warunków i możliwości danego obiektu

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

2.2 Instalacja uchwytów i wisiędników antenowych - (min. 200kpl.)

W celu zapewnienia możliwości podłączenia do budowanej infrastruktury Beneficjentów projektu oraz jednostek podległych (w których nie planuje się lokalizacji infrastruktury określonej wyżej), należy wykonać instalacje w postaci uchwytów lub wisiędników antenowych

Należy zaprojektować i wykonać wisiędniki 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 właścicielami lub administratorami poszczególnych budynków.

Wymagania ogólne

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

Wymagania gwarancyjne i serwisowe

- a) Wykonawca udzieli minimum 36 miesięcznej gwarancji na wykonane konstrukcje.
- b) W okresie gwarancji wykonawca zobowiązuje się do usuwania wszelkich wad i nieprawidłowości powstałych na wskutek normalnej eksploatacji.

- c) Jeżeli w trakcie okresu gwarancyjnego, istnieje konieczność wykonywania okresowych przeglądów gwarancyjnych, wówczas przeglądy te będą wykonywane na koszt Wykonawcy.

2.3 Instalacja szaf teletechnicznych oraz wykonanie instalacji okablowania zasilającego, sygnałowego oraz logicznego pod potrzeby instalacji wyposażenia węzłów sieci.

We wszystkich lokalizacjach budowy wież i/lub masztów 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.

3. **Budowa sieci szkieletowej oraz dystrybucyjnej (w oparciu o radiolinie cyfrowe i połączenia WLAN).**

Szkielet sieci powinien być oparty o cyfrowe radiolinie klasy operatorskiej o minimalnej przepustowości 100 Mb/s FDD, pracujące w szerokim zakresie częstotliwości: 11,13,18,28,32,38 GHz (poprzez dobór odpowiedniego ODU).

Szkielet sieci powinien być zapewnić połączenie o wysokiej przepustowości i dostępności dla instalowanych węzłów dystrybucyjnych i dostępowych sieci (bezprzewodowych punktów dostępu)

Planowana jest budowa min. 4 Węzłów Rdzeniowych sieci.

Ze względu na ukształtowanie terenu Gminy, istnieje konieczność budowy dodatkowych połączeń dystrybucyjnych punkt-punkt o mniejszej przepustowości. Dla zachowania efektywności ekonomicznej, zakłada się instalację połączeń dystrybucyjnych w oparciu o technologię IEEE 802.11a/n (MIMO), z wykorzystaniem nielicencjonowanego pasma radiowego 5 GHz. Planowana jest budowa min. 6 Węzłów Dystrybucyjnych sieci.

Dokładna ilość wymaganych połączeń dystrybucyjnych, będzie znana po przeprowadzeniu planowania radiowego oraz opracowaniu projektu wykonawczego sieci.

3.1 Radiolinie cyfrowe 100Mb/s FDD (min. 4kpl.)

Wymagania ogólne

- Wykonawca jest zobowiązany do opracowania dokumentacji projektowej w zakresie budowy sieci szkieletowej, której elementem będzie 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

- Wykonawca zobowiązany jest tak dobrać konfigurację radiolinii aby opłaty wnoszone do UKE przez Zamawiającego za wykorzystane pasmo radiowe były w okresie trwałości projektu minimalne

Wymagania techniczne:

- Część wewnętrzna radiolinii (IDU) musi mieć możliwość współpracy z systemem zewnętrznymi jednostkami radiowymi (ODU) mogących pracować w następujących pasmach: 13, 18, 23, 28, 32, 38 GHz
- Radiolinia musi 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
- Dla kanału 7Mhz i modulacji 256 QAM radiolinia musi umożliwiać uzyskanie przepływności min. 50 Mb/s FDX (full duplex)
- Automatyczna regulacja Mocy nadajnika (ATPC)
- Radiolinia musi 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, CNT400 lub równoważnego
- Zasilanie: napięcie standardowe -48 VDC
- 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 400 Mb/s FDX dla trybu 256QAM w kanale 56MHz (bez zmiany lub dodania jakiegokolwiek części sprzętowej, jedynie poprzez zmianę klucza licencyjnego)
- Wymaga się aby radiolinia była wyposażona w następujące interfejsy zewnętrzne (możliwe do przeznaczenia na transmisję ruchu) w minimalnej liczbie:
 - 2x10/100/1000Base-T – elektryczny
 - 2 x gniazdo SFP z możliwością dołączenia optyki niezależnego producenta
- 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

Wymagania gwarancyjne i serwisowe

- Urządzenia powinny być objęte minimum 36 miesięczną gwarancją producenta.
- W okresie gwarancji (36 miesiące) Wykonawca powinien zapewnić gotowość serwisową polegającą na naprawie lub podmianie sprzętu w razie awarii, najpóźniej następnego dnia roboczego, od momentu zgłoszenia usterki.

3.2 Połączenia dystrybucyjne punkt-punkt - (min. 8kpl.)

Warstwa dystrybucyjnej sieci zostanie zbudowana w oparciu o połączenia dystrybucyjne punkt-punkt zgodnie ze standardem IEEE 802.11a/n (MIMO). Planowana jest instalacja min. 8 takich połączeń. Zadaniem tej warstwy jest dostarczanie wysokiej jakości usług transmisji danych oraz dostępu do Internetu. Ponadto dzięki możliwości implementacji mechanizmów QoS (Quality of Service), zachowana zostanie wysoka dostępność i jakość usług. Za pomocą połączenia dystrybucyjnego planowane jest podłączenie tych Jednostek Podległych, w których planuje się instalację bezprzewodowych punktów dostępu. W pozostałych przypadkach dopuszcza się przyłączenie Jednostek do sieci za pomocą terminali końcowych. Tabela poniżej zawiera listę wszystkich Jednostek Podległych objętych projektem.

Ip	Nazwa Jednostki Podległej	Adres
1	Szkoła Podstawowa w Poraju,	Górnicza 18
2	Szkoła Podstawowa w Kuźnicy Starej,	Kuźnica Stara 43
3	Szkoła Podstawowa w Żarkach Letnisko,	Szkolna 20
4	Gimnazjum w Poraju,	Górnicza 18

5	Gimnazjum w Żarkach Letnisko,	Szkolna 20
6	Przedszkole w Poraju,	Jasna 14
7	Przedszkole w Żarkach Letnisko,	Szkolna 20
8	Gminna Biblioteka Publiczna w Poraju,	Piłsudskiego 14
9	Biblioteka Publiczna w Poraju - filia w Kuźnicy Starej,	Kuźnica Stara 43
10	Biblioteka Publiczna w Poraju - filia w Żarkach Letnisko,	Szkolna 20
11	Gminny Ośrodek Kultury w Poraju,	Piłsudskiego 14
12	Gminny Ośrodek Zdrowia w Poraju,	3-go Maja 25
13	Gminny Ośrodek Pomocy Społecznej,	Górnicza 21
14	ZEAS	Górnicza 18

Wymagania techniczne

- Urządzenie przeznaczone do zastosowań zewnętrznych typu punkt-punkt (wyposażone w zestaw montażowy),
- Temperatura pracy: od -30C do 75C,
- Wilgotność pracy: 5 to 95%,
- Pamięć: 64MB SDRAM, 8MB Flash,
- 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,
- Regulacje prawne: 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 802.11a/n 2x2 MIMO o zwiększonej wydajności odbiornika i realnej wydajności min. 150 Mbps dla ruchu TCP/IP,
- Pracuje w trybach: router lub bridge,
- Interfejsy WiFi wspierający tryby Access Point, Access Point WDS, Client, Client WDS.
- System do centralnego zarządzania min. 100 urządzeniami

3.3 Przełączniki dystrybucyjne 24 porty 10/100, (min. 4 szt.)

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 (timedomainreflector)
- 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 (ratelimiting) 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. protectedports) 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 SpanningTree 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 nową 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

4. Budowa sieci dostępowej (Węzłów Dostępowych oraz instalacji terminali odbiorczych)

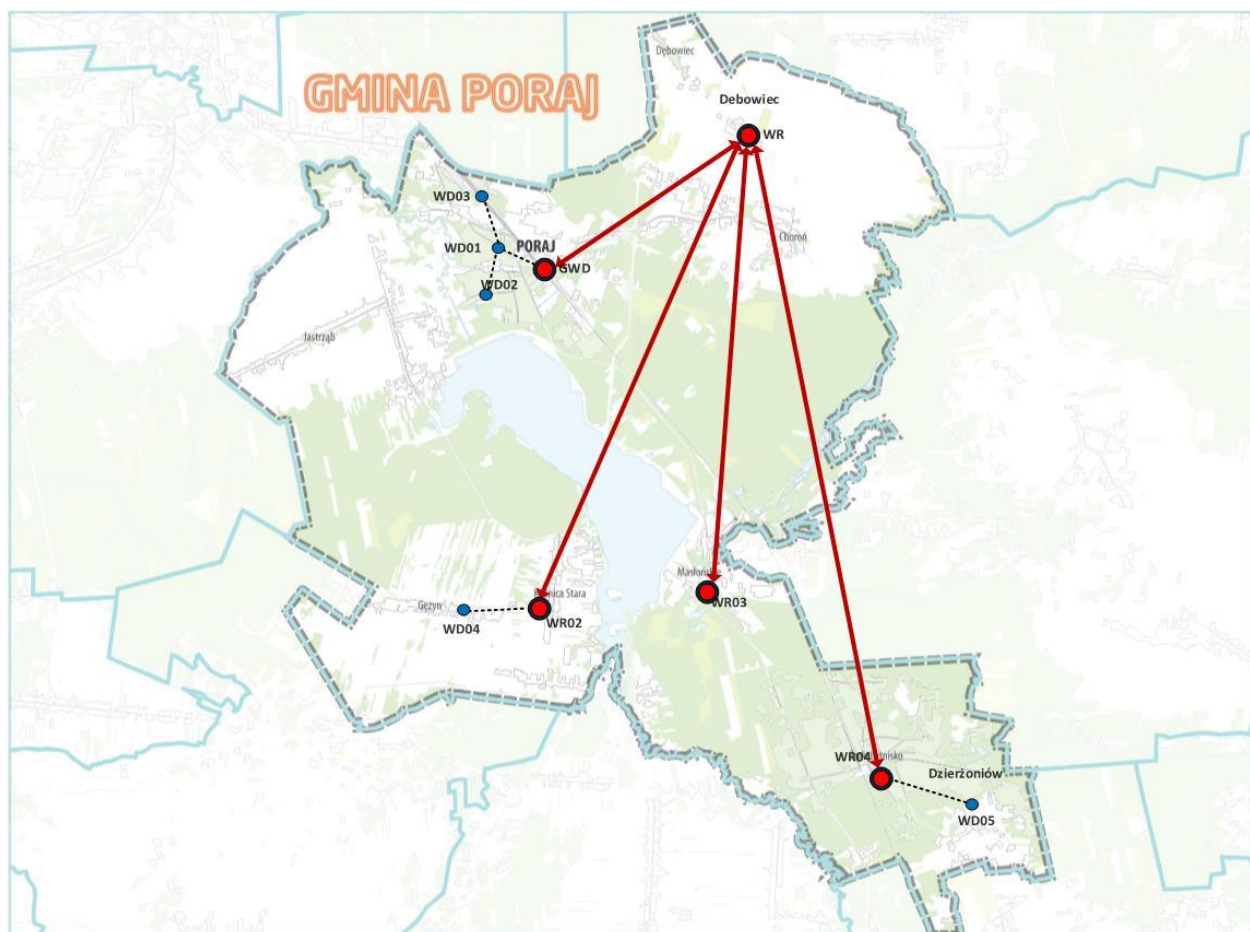
Wymagana jest instalacja węzłów dostępowych, z odpowiednim wyposażeniem i funkcjonalnością i w ilości wynikającej z planowania radiowego oraz potrzeb pojemności sieci, jednak nie mniej niż 10kpl. W pojedynczej lokalizacji Węzła Dostępowego będzie zainstalowany bezprzewodowy punkt dostępowy (jeden lub kilka w zależności od warunków terenowych) oraz inne elementy i urządzenia zapewniające odpowiednią funkcjonalność, zgodnie ze specyfikacją określoną w dalszej części rozdziału.

Lokalizację węzłów dostępowych, należy zaplanować w taki sposób, aby zapewnić optymalne pokrycie sygnałem radiowym miejscowości objętych projektem (zgodnie z poniższą specyfikacją). Instalowane węzły dostępne powinny zapewnić możliwość podłączenia Beneficjentów projektu (gospodarstw domowych) w miejscowościach objętych projektem tj.:

L.P.	Nazwa miejscowości objętych projektem
1.	Dębowiec
2.	Dzierżno
3.	Żarki-Letnisko
4.	Gęzyn
5.	Masłońskie
6.	Kuźnica Stara
7.	Poraj

Projekt zakłada, że węzły dostępne (stacje bazowe) będą instalowane na istniejących obiektach (budynkach) jednostek podległych Gminy i często ich lokalizacja będzie się pokrywać z lokalizacją węzłów dystrybucyjnych czy rdzeniowych. Dopuszczalne jest również wykorzystanie innych budynków i obiektów należących do Gminy Poraj, należy jednak pamiętać, że budowa węzłów dostępowych sieci jest dopuszczalna wyłącznie we wskazanych wyżej miejscowościach.

Na rysunku poniżej przedstawiono przykładowy schemat rozmieszczenia węzłów sieci



Przykładowy schemat rozmieszczenia węzłów sieci

Uwaga!

Zaleca się dokonanie wizji lokalnej we wszystkich lokalizacjach, w których planowana jest instalacja węzłów dostępowych w celu prawidłowego wyliczenia kosztów związanych z ich budową. Zamawiający na prośbę wykonawcy udostępni pełną listę wszystkich jednostek podległych Gminy Poraj. Lokalizacja szaf dystrybucyjnych, sposób prowadzenia instalacji zasilającej i sygnałowej powinien być wcześniej uzgodniony z właścicielem obiektu.

Wszystkie węzły dostępowe powinny być wyposażone w następujący zestaw elementów i urządzeń:

a) w zakresie infrastruktury pasywnej:

- wysięgniki i konstrukcje wsporcze pod anteny
- szafka dystrybucyjna 19"
- okablowanie zasilające do szaf
- okablowanie logiczne

b) w zakresie infrastruktury aktywnej

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

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

4.1 Przełączniki dostępowe 8 port 10/100 8xPoE –(w ilości odpowiadającej ilości węzłów dostępowych, jednak nie mniej niż 10 szt.)

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 (WeightRound Robin) / CoS (Class of Service) dla 4 kolejek na każdym porcie przełącznika:
 - Port-based,
 - 802.1p VLAN prioritybased,
 - 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 aktualizacji firmware'u (TFTP, przeglądarka internetowa HTTP),

- inne opcje zarządzania - Telnet (Menu-driven configuration):
 - Secure Shell (SSH),
 - RADIUS,
 - TACACS,
 - Telnet Client,
 - SecureSocketLayer (SSL),
 - Switch Audit Log,
 - DHCP Client,
 - BootP,
 - SNTP,
 - Xmodemupgrade,
 - 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),
- stormcontrol: możliwość ograniczenia rozsyłania ramek broadcast / multicast / unknownunicast,
- 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%,

4.2 UPS 1000VA RACK - (w ilości odpowiadającej ilości węzłów dostępowych, jednak nie mniej niż 10 szt.)

Wymagania techniczne

- Moc pozorna 1000VA
- Moc rzeczywista 600 Wat
- Architektura UPSaline-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 powinny posiadać obudowę typu Rack 19"
- Maksymalna wysokość urządzenia 2U

4.3 Bezprzewodowy punkt dostępu 802.11a/b/g/n 2x2 MIMO (w ilości nie mniej niż 20 szt.)

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 Dynamicznywybórkanalu (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)
 - ✓ 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:
 - ✓ Sieć Ethernet zgodnie ze standardemIEEE 802.3af PoE
 - ✓ Lokalny zasilacz
- Pobór mocy: max. 16 Watt,
- Powinno posiadać solidną metalową obudowę
- Temperatura pracy: od -20C do 55C,
- Praca w warunkach wilgotności: 10 do 90%,

4.4 Anteny do punktów dostępowych MIMO - MIMO (w ilości odpowiadającej ilości bezprzewodowych punktów dostępowych, jednak nie mniej niż 40 szt.)

Dobór rodzaju oraz typów anten, powinien być uzależniony od warunków propagacyjnych dla poszczególnych lokalizacji, w których zostaną zainstalowane bezprzewodowe punkty dostępu. Należy jednak stosować anteny sektorowe i/lub dookólne, wykonane w technologii MIMO 2x2 i przystosowane do zastosowań zewnętrznych. Każdy bezprzewodowy punkt dostępu należy wyposażyć w anteny na pasmo radiowe 2,4 GHz, jak i 5 GHz (praca równoległa).

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

4.5 Bezprzewodowy terminal klienta 802.11 a/n

Wymagania techniczne dla terminali klienta 802.11 a/n

Interfejsy

- Interfejs Ethernet : 100 base-T Ethernet (RJ-45) zgodny z PoE
- LAN Protokół : IEEE 802.3 (CSMA/CD)
- WLAN Protokół Radiowy: IEEE 802.11a/n
- Interfejs WLAN : OFDM, TDD

Radio

- Zakres obsługiwanych częstotliwości: Europa (ETSI): 5500-5700 MHz (11 kanałów) zDFS (automatyczny wybór częstotliwości),
 - Typ modulacji : BPSK, QPSK, 16QAM, 64QAM, HT20, HT40
 - Szerokość kanału możliwość ustawienia : 5 / 10 / 20 /40 MHz
 - Moc wyjściowa : < 30 dBm EIRP
 - Zintegrowana antena panelowa dual polar 15 dBi
- Inne cechy
- Temperatura pracy : -30°C - +70°C

4.6 Bezprzewodowy terminal klienta 802.11 b/g/n

Wymagania techniczne dla terminali klienta 802.11 b/g/n

Interfejsy

- Interfejs Ethernet : 100 base-T Ethernet (RJ-45) zgodny z PoE
- LAN Protokół : IEEE 802.3 (CSMA/CD)
- WLAN Protokół Radiowy: IEEE 802.11 b/g/n
- Interfejs WLAN : OFDM, TDD

Radio

- Zakres obsługiwanych częstotliwości: Europa (ETSI): 2400-2483,5 MHz (13 kanałów)
 - typ modulacji : BPSK, QPSK, 16QAM, 64QAM, HT20, HT40
 - Szerokość kanału możliwość ustawienia : 5 / 10 / 20/40 MHz
 - Moc wyjściowa : < 20 dBm EIRP
 - Zintegrowana antena panelowa dual polar 14 dBi
- Inne cechy
- Temperatura pracy : -30°C - +70°C

Uwaga!

Sumaryczna liczba terminali Klientkich określonych w punkcie 4.5 i 4.6 powinna wynosić min. 200 szt.

5. Wyposażenie Głównego Węzła Dystrybucyjnego i Centrum Zarządzania siecią szerokopasmową.

5.1 Adaptacja pomieszczenia Centrum Zarządzania siecią szerokopasmową

Planowane jest wykorzystanie jednego z pomieszczeń w budynku Urzędu Gminy Porajna Główny Węzeł Dystrybucyjny oraz Centrum Zarządzania siecią. Pomieszczenie przeznaczone na lokalizację GWD i CZ będzie wymagało wykonania prac adaptacyjnych w zakresie:

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

- 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 zbitcia 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 klucz. Manipulator oraz kasetka 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 weryfikację 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 zablożenia powinna reagować na zdarzenia niepożądanego dostępu poprzez zastosowanie czujników ruchu, otwarcia drzwi, zbitcia 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 alarmowania 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 gwarancyjne i serwisowe

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

5.2 Przełącznik rdzeniowy L3 (min. 1 szt.)

Wymagania techniczne:

- Przełącznik o zamkniętej konfiguracji, posiadający 24 porty GigabitEthernet 10/100/1000Base-T oraz 4 gniazda typu SFP pozwalające na instalację wkładek z portami Gigabit Ethernet 1000BASE-T, 1000BASE-SX, 1000BASE-ZX, 1000BASE LX/LH.
- Przełącznik musi posiadać, co najmniej 128 MB pamięci DRAM oraz 32 MB pamięci Flash
- Dostępne w przełączniku gniazda SFP powinny umożliwiać instalację modułów dla wielokrotnionej transmisji optycznej CDWM
- Przełącznik musi posiadać wydajność przełączania przynajmniej 38 Mpps dla 64-bajtowych pakietów;
- Przełącznik musi zapewniać obsługę 12,000 adresów MAC, 11,000 tras w tablicy routingu oraz 1024 sieci VLAN
- Przełącznik musi współpracować z modułem redundantnego zewnętrznego zasilacza.
- Przełącznik musi zapewniać przełączanie w warstwie drugiej.
- Przełącznik musi umożliwiać przełączanie w warstwie trzeciej oraz definiowanie routingu w oparciu o protokoły RIPv1, RIP v2, OSPF i BGPv4 oraz routing statyczny.
- Przełącznik musi zapewniać obsługę ruchu IP Multicast, protokoły PIM Sparse oraz PIM Dense, funkcjonalność IGMP Snooping.
- Przełącznik musi posiadać możliwość uruchomienia funkcjonalności DHCP: DHCP Server oraz DHCP Relay
- Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
 - a. IEEE 802.1s Rapid Spanning Tree
 - b. IEEE 802.1w Multi-Instance Spanning Tree
 - c. możliwość grupowania portów zgodnie ze specyfikacją IEEE 802.3ad (LACP)
- Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
 - a. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
 - b. Implementacja co najmniej czterech kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu Round Robin lub podobnego dla obsługi tych kolejek

- c. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (StrictPriority)
- d. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP.
- Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
 - a. Wiele poziomów dostępu administracyjnego poprzez konsolę
 - b. Autoryzacja użytkowników/portów w oparciu o IEEE 802.1x
 - c. Możliwość uzyskania dostępu do urządzenia przez SNMPv3 i SSHv2
 - d. Funkcjonalność prywatnego VLAN-u, czyli możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. porty izolowane) z pozostawieniem możliwości komunikacji z portem nadrzędnym
- Przełącznik powinien umożliwiać lokalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu
- Przełącznik powinien umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN
- Przełącznik powinien mieć możliwość synchronizacji zegara czasu za pomocą protokołu NTP
- Przełącznik powinien posiadać możliwość połączenia z innymi przełącznikami tego samego typu w klastery zapewniający możliwość zarządzania za pomocą pojedynczego adresu IP
- Urządzenie powinno umożliwiać zarządzania poprzez interfejs CLI (konsolę).
- Plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) 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 musi być możliwe uruchomienie urządzenia z nową konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu
- Musi mieć możliwość montażu w szafie 19", wysokość nie większą niż 1RU;

5.3 Urządzenie bezpieczeństwa sieciowego (1 szt.)

Wymagania techniczne

- Urządzenie powinno pełnić rolę ściany ogniowej śledzącej stan połączeń
- Powinno być oparte o dedykowany 64 bitowy system operacyjny pracujący na procesorze wielordzeniowym
- Urządzenie nie powinno posiadać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej
- Urządzenie musi posiadać co najmniej 6 portów GigabitEthernet RJ-45, port GigabitEthernet dla zarządzania i port konsoli RJ-45
- Urządzenie powinno posiadać dodatkowy slot do rozbudowy o dodatkowe minimum 6portów RJ-45 zamienne z modułami optycznymi SFP.
- Powinno posiadać co najmniej porty USB
- Powinno posiadać co najmniej 4 GB DRAM oraz 4 GB Flash
- Urządzenie musi posiadać zintegrowane sprzętowe wsparcie dla szyfrowania
- Urządzenie powinno umożliwiać funkcjonalność IPS w postaci modułu programowego pracującego pod kontrolą 64 bitowego systemu operacyjnego po wykupieniu dodatkowej licencji
- Urządzenie powinno mieć możliwość ochrony przed sieciami Botnet.
- Urządzenie powinno mieć możliwość uruchamiania nowych usług bezpieczeństwa bez potrzeby stosowania dodatkowego sprzętu
- Urządzenie powinno mieć możliwość operowania jako transparentna ściana ogniowa warstwy drugiej ISO OSI
- Urządzenie powinno umożliwiać terminowanie co najmniej 250 jednoczesnych sesji VPN opartych o protokół IPSec

- Na urządzeniu musi istnieć możliwość terminowania jednocześnie do 250 sesji WebVPN przy zastosowaniu odpowiedniej licencji na oprogramowanie
- Urządzenie powinno obsługiwać co najmniej 100 000 jednoczesnych sesji/połączeń z prędkością 15 000 nowych połączeń na sekundę
- Przepustowość firewall obsługiwana przez urządzenie nie musi być mniejsza niż 1 Gbps, 250 Mbps dla ruchu z włączoną kontrolą IPS i 200 Mbps dla ruchu szyfrowanego symetrycznymi algorytmami 3DES/AES
- Wraz z urządzeniem powinno być dostarczane oprogramowanie klienta VPN, umożliwiające instalację go i zestawienie do urządzenia połączeń VPN z komputerów osobistych PC pracujących pod kontrolą systemów operacyjnych Windows, Solaris i Linux, a także komputerów Mac. Oprogramowanie to powinno pochodzić od tego samego producenta, co oferowane urządzenie i powinno być objęte jego jednolitym wsparciem technicznym.
- Urządzenie powinno umożliwiać obsługę co najmniej 50 interfejsów VLAN w standardzie 802.1
- Urządzenie powinno w celu redundancji umożliwiać implementację funkcji niezawodności pary takich urządzeń, czyli tzw. failoveru działającego w trybie active/standby oraz active/active
- Urządzenie powinno umożliwiać rozbudowę do obsługi co najmniej 5 wirtualnych instancji firewall
- Powinno obsługiwać protokoły routingu OSPF, RIP, PIM
- Urządzenie powinno realizować kompresję protokołów DTLS i TLS
- Urządzenie powinno dokonywać inspekcji protokołów RTSP, TFTP, DNS, FTP, GTP, HTTP, ICMP, PPTP, SMTP, ESMTTP
- Powinno dokonywać inspekcji ruchu głosowego w zakresie protokołów H.323, SIP, SCCP, CTIQBE, MGCP, TAPI, JTAPI, RTSP
- Urządzenie powinno dokonywać inspekcji protokołów bazodanowych ISL, SQL*Net, Sun RPC
- Urządzenie powinno dokonywać inspekcji protokołów zarządzających DCERPC, GTP, RADIUS, RSH, SNMP, XDMCP
- Urządzenie powinno mieć możliwość realizacji funkcji Phone Proxy
- Urządzenie powinno zapewniać wsparcie dla list kontroli dostępu dla IPv6
- Urządzenie powinno być zarządzalne przy wykorzystaniu dedykowanej aplikacji umożliwiającej płynną (z użyciem kreatorów) konfigurację poszczególnych funkcji urządzenia.
- Urządzenie dostosowane do pracy w zakresie temperatur minimum od -5 do 40 °C, przy wilgotności do 90 procent, pobór mocy nie więcej niż 65 W
- Urządzenie powinno być przystosowane do montażu w 19-calowej szafie rackowej i nie zajmować więcej miejsca niż 1RU (rack unit)

5.4 Kontroler sieci bezprzewodowej WLAN (1 szt.)

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. 25 punktami dostępowymi z możliwością licencyjnej rozbudowy systemu do 500 punktów dostępowych
- min. 8 styków definiowanych przez moduły typu SFP zgodnymi ze standardami 1000Base-T, 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 SNMP
- 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

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

Wymagania techniczne:

- Moc pozorna 3000VA
- Moc rzeczywista 1800 Wat

- Architektura UPSaline-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 baterijnego
- Urządzenia powinno posiadać obudowę typu Rack 19"
- Maksymalna wysokość urządzenia wraz z baterią nie może przekroczyć 6U

5.6 Szafa 42U z wyposażeniem (1 szt.)

Wyposażenie

Szafa serwerowa 42U szer:800 głęb: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

5.7 Serwery i urządzenia dodatkowe

Wymagania techniczne (sprzętowe oraz systemowe):

5.7.1 Platforma do wirtualizacji środowisk serwerowych –serwer (1 szt.)

Serwer sieciowy przeznaczony do zapewnienia usług dostępowych dla Beneficjentów sieci	
Nazwa komponentu	Wymagane minimalne parametry techniczne
Procesor	Zainstalowany jeden procesor dedykowany do pracy w serwerach, uzyskujący w teście wydajności Passmark CPU Mark wynik min. 9600 punktów. Wydruk ze strony internetowej http://www.cpubenchmark.net dla oferowanego procesora (nie starszy niż na dzień 01.09.2014r.) należy dołączyć do oferty Możliwość rozbudowy do wersji dwu-procesorowej
Pamięć	min. 16GB pamięci operacyjnej (możliwość rozbudowy do 144GB)
Pamięć masowa	Zainstalowany kontroler SAS 2.0 RAID 0,1,5,6,50,60, 1GB pamięci podręcznej z podtrzymaniem baterijnym Zainstalowane 3 dyski SAS 2.0 Hotplug o pojemności 300 GB każdy - możliwość obsadzenia do 8 wnęk dyskami twardymi Hotplug2,5" - obsługa dysków SAS, SATA, SSD;
Grafika	Zintegrowana ze złączem VGA
Napędy wbudowane	Nagrywarka DVD +/-RW
Funkcjonalność płyty głównej	- możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora (niezależne od dysków twardych) - wbudowane 2x 1Gb/s LAN, z obsługą iSCSI, iSCSIboot, teamingu, RJ-45
Funkcjonalność obudowy	Rack19", max. wysokość 2U - dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy rack oraz ramieniem porządkującym ułożenie przewodów w szafie rack; - dwa redundantne zasilacze hotplug o sprawności 94% i mocy maksymalnej 460W; - redundantne wentylatory hotplug;
Oprogramowanie	- Serwerowy system operacyjny spełniający następujące wymagania poprzez

	<p>wbudowane mechanizmy, bez konieczności użycia dodatkowych aplikacji.</p> <ul style="list-style-type: none"> - Graficzny interfejs użytkownika - Obsługa systemów wieloprocesorowych - Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu - Możliwość implementacji następujących funkcjonalności: <ul style="list-style-type: none"> o Podstawowe usługi sieciowe: DNS, DHCP o Usługi katalogowe pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe) o Zdalna dystrybucja oprogramowania na stacje robocze o Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej o PKI (Centrum Certyfikatów, obsługa klucza publicznego i prywatnego) o Szyfrowanie plików i folderów o Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec) o Serwis udostępniania stron WWW o Serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management) o Wsparcie dla protokołu IP w wersji 6 (IPv6) o Wbudowane mechanizmy wirtualizacji o Możliwość uruchomienia 1 maszyny wirtualnej w ramach licencji na serwer - Wbudowana zaporą ogniową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych - Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe - Wsparcie dla urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play) - Licencja na połączenie do zasobów serwera min. 5 użytkowników - Zorganizowany system szkoleń i materiały edukacyjne w języku polskim
Bezpieczeństwo	<p>Serwer musi posiadać:</p> <ul style="list-style-type: none"> - zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania (zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego)
Zarządzanie	<p>Wbudowany wyświetlacz diagnostyczny informujący o stanie serwera; Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:</p> <ul style="list-style-type: none"> - niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; - dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; - dostęp poprzez przeglądarkę Web (także SSL, SSH) - zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii - zarządzanie alarmami (zdarzenia poprzez SNMP) - możliwość przejęcia konsoli tekstowej - przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) - oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (min. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna)
Wymagania	<p>Zintegrowane w obudowie:</p>

dodatkowe	- Porty USB: min. 7 gniazd, w tym min. 2 z przodu obudowy - Gniazdo RS232
Certyfikaty standardy	- ISO9001 lub równoważny dla producenta serwera, - Deklaracja zgodności CE
Wsparcie techniczne	- Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta, jego przedstawiciela lub Wykonawcy. - Dostęp do najnowszych sterowników i uaktualnień realizowany poprzez podanie na dedykowanej stronie internetowej numeru seryjnego lub modelu komputera
Gwarancja	
Kompletny zestaw	3 lata gwarancji świadczonej w miejscu eksploatacji sprzętu - czas reakcji serwisu - do końca następnego dnia roboczego - w przypadku awarii komputerowych dysków twardych - dysk uszkodzony pozostaje u Zamawiającego - dostępność części zamiennych przez okres min. 5 lat od zakupu serwera

Wymagania ogólne dotyczące instalacji oprogramowania na serwerze:

Na dostarczonym serwerze należy zainstalować oraz skonfigurować następujące oprogramowanie:

- instalacja oraz konfiguracja środowiska wirtualizacji serwerów Hyper-V
- instalacja oraz konfiguracja systemu do scentralizowanego zarządzania infrastrukturą maszyn wirtualnych
- utworzenie oraz konfiguracja maszyny wirtualnej dla systemu monitoringu stanu sieci
- dostawa, instalacja oraz konfiguracja systemu będącego środowiskiem dla oprogramowania spełniającego funkcje systemu Monitoringu na maszynie wirtualnej
- utworzenie oraz konfiguracja maszyny wirtualnej dla systemu LMS (ang. *LanManagement System*; System Zarządzania Siecią)
- dostawa, instalacja oraz konfiguracja systemu będącego środowiskiem dla oprogramowania LMS na maszynie wirtualnej
- utworzenie oraz konfiguracja maszyny wirtualnej dla systemu zarządzania pasmem
- dostawa, instalacja oraz konfiguracja systemu będącego środowiskiem dla oprogramowania „TrafficManager”

a) System monitoringu infrastruktury sieciowej (1 kpl.)

Wymagania funkcjonalne systemu monitoringu stanu sieci:

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

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

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

Wymagania funkcjonalne systemu LMS:

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

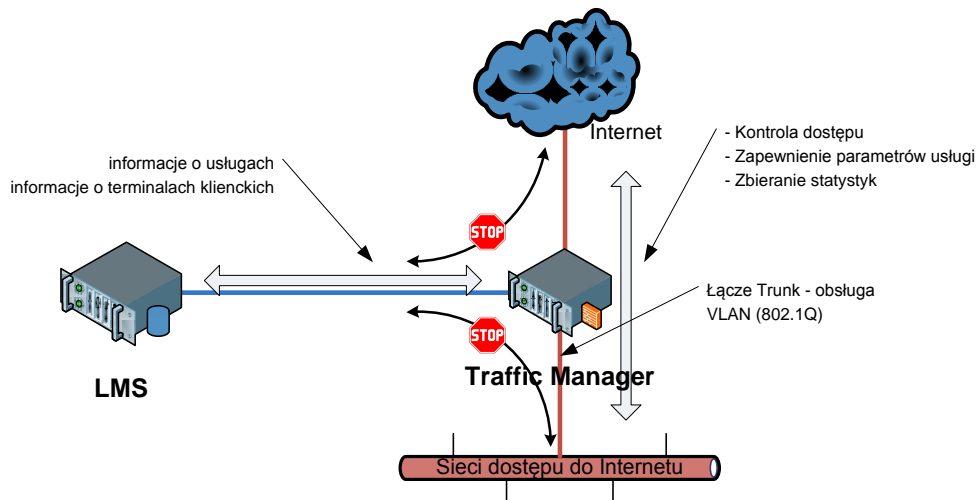
System ten powinien cechować się następującą funkcjonalnością:

- wszelkie dane systemu takie jak: definicje usług, użytkowników, administratorów, urządzenia oraz adresacji sieci przechowywane w bazie SQL
- udostępniona dokumentacja wraz z strukturą drzewa bazy
- dane bazy udostępnione i wykorzystywane przez wszystkie elementy składowe systemu LMS
- przyjazny intuicyjny graficzny interfejs zrealizowany w technologii WWW - udostępniony w sieci zarządzania poprzez protokół http/https
- zarządzanie dostępem do usług (w tym kontrola pasma i statystyk, możliwość prostego włączenia/wyłączenia dostępu do usługi) – tworzenie taryf z definicją parametrów upload/download, ilość połączeń na sekundę, limit danych
- współpraca z zaproponowanym systemem „TrafficManager” – generowanie kolejki ruchu w oparciu o zdefiniowane w bazie usługi oraz „klientów” sieci
- ewidencja sprzętu sieciowego – urządzeń sieci (nazwa, model, producent, numer seryjny, hasładostępu, data zakupu, okres gwarancji, iloscportow, 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, protokoły)
- korespondencja seryjna
- zarządzanie kontami oraz hostingiem np. kona pocztowe,
- zarządzanie informacja o dodatkowych usługach: mail, ftp, voip itp.
- system obsługi zgłoszeń oraz wyjazdów serwisowych
- archiwizacja danych
- platforma kontaktu z abonentem
- zarządzanie administratorami oraz prawami dostępu do poszczególnych funkcjonalności systemu
- możliwość prostego wyszukiwania urządzeń, adresów IP czy klientów
- serwer typu RADIUS pozwalający na autentykację w oparciu o dane z bazy danych SQL

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

Wymagania funkcjonalne systemu „TrafficManager”:

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



Oprogramowanie musi posiadać następujące cechy i funkcje:

- Kontrola dostępu – nakładanie polityki uprawnień dostępu
 - ✓ sprawdzenie poprawności adresu MAC, IP
 - ✓ zabronienie dostępu odłączonym klientom
 - ✓ możliwość autentykacji użytkownika na podstawie logowania WWW lub PPPoE z użyciem par użytkownik/hasło z bazy danych LMS
 - ✓ wyświetlanie komunikatów w przeglądarce WWW
- Zapewnienie parametrów jakościowych zdefiniowanej w systemie 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 definicją 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 przysyłających SPAM
- Tworzenie graficznych statystyk transferów (sieci oraz indywidualnych użytkownika) oraz obciążenia zasobów systemu
- Zabezpieczenia dostępu do sieci
 - ✓ kontrola dostępu terminali klienckich
 - ✓ odseparowanie ruchu sieci zarządzania od sieci klienckich oraz sieci Internet
 - ✓ konfiguracja blokad ruchu z sieci klienckich oraz Internet do panelów zarządzania systemem TrafficManager
 - ✓ konfiguracja blokad ruchu między sieciami klienckimi
 - ✓ ochrona przed atakami DoS
 - ✓ zabezpieczenia przed skanowaniem portów i nieautoryzowanym dostępem
- automatyczny backup konfiguracji, możliwość łatwego eksportu/importu konfiguracji z poziomu graficznego panelu administracyjnego

5.7.2 Dostawa i instalacja systemu pamięci masowej

System NAS stanowiący centralny magazyn danych i kopii zapasowych dla systemów fizycznych i maszyn wirtualnych	
Nazwa komponentu	Wymagane minimalne parametry techniczne
Wydajność	Procesor dedykowany do pracy w komputerach typu embedded, uzyskujący w teście Passmark CPU Mark wynik min. 800 punktów. Wydruk ze strony internetowej http://www.cpubenchmark.net dla oferowanego procesora (nie starszy niż na dzień 01.09.2014r.) należy dołączyć do oferty
Pamięć	nieulotna 128 MB typu Flash, operacyjna 1 GB
Pamięć masowa	<ul style="list-style-type: none"> - dostępne 4 kieszenie hot-swap z możliwością fizycznej blokady - zainstalowane 4 dyski hot-swap dedykowane do pracy w serwerach, każdy po 2TB - bezpieczeństwo na poziomie RAID 0/ 1/ 5/ 6/ 5+ hot spare, JBOD - system plików ext3, ext4 (dyski wewnętrzne), ext3, ext4, NTFS, FAT32, HFS+ (dyski zewnętrzne)
Interfejsy	<ul style="list-style-type: none"> - 2 x Gigabit Ethernet z obsługą iSCSI - 3 x USB 2.0 - 1x USB 3.0
Funkcjonalność obudowy	<ul style="list-style-type: none"> - Rack 19", max. wysokość 1U dostarczona wraz z szynami umożliwiającymi wysunięcie serwera z szafy rack - dwa redundantne zasilacze
Obsługiwane protokoły	TCP/IP, DHCP client, DHCP server, CIFS/SMB, AFP, NFS, HTTP, HTTPS, FTP, DDNS, NTP, wsparcie Gigabitowych ramek Jumbo, ustawienia Multi-IP, równoważenie obciążenia, Network Service Discovery (UPnP&Bonjour)
Zarządzanie	ograniczenie dostępnej pojemności dysku dla użytkownika, integracja z usługami domenowymi, zarządzanie kontami użytkowników (maksymalnie 4096 użytkowników), zarządzanie grupą użytkowników (maksymalnie 512 grup), tworzenie zestawów użytkowników
Oprogramowanie	<ul style="list-style-type: none"> - Dedykowany system operacyjny typu embedded, - Dodatkowe oprogramowanie do tworzenia obrazów dysku, przywracania systemu od podstaw, szybkiego odzyskiwania bez konieczności ponownego instalowania systemu operacyjnego i aplikacji, zawierające: <ul style="list-style-type: none"> - rozbudowane funkcje katalogowania do łatwego przeglądania, wyszukiwania i przywracania różnych wersji poszczególnych plików z kopii zapasowych obrazów - szybkie, jednoczesne, bezagentowe operacje tworzenia kopii zapasowych i odzyskiwania maszyn wirtualnych - możliwość tworzenia kopii zapasowych i odzyskiwania danych na nieograniczonej liczbie maszyn wirtualnych działających na hoście, a także wykonywanie migracji typu V2P i P2V
Gwarancja	
Kompletny zestaw	<ul style="list-style-type: none"> 3 lata gwarancji świadczonej w miejscu eksploatacji sprzętu - czas reakcji serwisu - do końca następnego dnia roboczego - w przypadku awarii komputerowych dysków twardych - dysk uszkodzony pozostaje u Zamawiającego

5.7.3 Dostawa i instalacja stacji do zarządzania

Komputer typu All-in-One przeznaczony do zadań administracyjnych, dedykowany do obsługi baz danych, programowania współbieżnego, dostępu do sieci Internet, aplikacji biurowych i grafiki prezentacyjnej	
Nazwa atrybutu	Wymagane minimalne
Wydajność	Procesor dedykowany do pracy w komputerach stacjonarnych, uzyskujący w teście Passmark CPU Mark wynik min. 6000 punktów.

	<p>Wydruk ze strony internetowej http://www.cpubenchmark.net dla oferowanego procesora (nie starszy niż na dzień 01.09.2014r.) należy dołączyć do oferty</p> <p>Komputer w oferowanej przez Wykonawcę konfiguracji testowany przy rozdzielczości wbudowanego ekranu min. 1920 x 1080 powinien osiągać w teście wydajności SYSMark2012 Web Development wynik co najmniej 160 pkt. (szczegółowy raport z przeprowadzonych testów należy dołączyć do oferty).</p>
Pamięć	<p>min. 4GB pamięci operacyjnej (możliwość rozbudowy do 16GB)</p> <p>min. 500GB pamięci masowej SATA</p>
Grafika	<p>Komputer w oferowanej przez Wykonawcę konfiguracji testowany przy rozdzielczości wbudowanego ekranu min. 1920 x 1080 powinien osiągać w teście wydajności SYSMark2012 3D Modeling wynik co najmniej 220 pkt. (szczegółowy raport z przeprowadzonych testów należy dołączyć do oferty).</p>
Napędy wbudowane	<p>Nagrywarka DVD +/-RW wraz z oprogramowaniem do nagrywania i odtwarzania płyt</p> <p>Czytnik kart multimedialnych</p>
Funkcjonalność BIOS	<p>Możliwość:</p> <ul style="list-style-type: none"> - skonfigurowania hasła „Power On” oraz ustawienia hasła dostępu do BIOSu (administratora) w sposób gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS, - ustawienia hasła na dysku - blokady/wyłączenia portów USB, COM, karty sieciowej, karty audio; - blokady/wyłączenia kart rozszerzeń/slotów PCI - kontroli sekwencji boot-owania; - startu systemu z urządzenia USB - blokowania boot-owania stacji roboczej z zewnętrznych urządzeń - ustawienia hasła na poziomie administratora bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych - automatycznej (lub na żądanie) aktualizacji BIOS przez sieć włączaną z poziomu BIOS przez użytkownika, bez konieczności uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.
Funkcjonalność obudowy	<ul style="list-style-type: none"> - typ All-in-One (komputer zintegrowany w obudowie wraz z monitorem) z ekranem LED antyodblaskowym IPS min. 21,5” FullHD (1920x1080) o kontraście typowym min.: 1000:1; jasności min.: 250 cd/m2, kątach widzenia min. 178 stopni (w pionie i poziomie) - dostępna regulacja kąta nachylenia ekranu (-5/+30 stopni), obrotowa podstawa (360 stopni) - zasilacz wewnętrzny o mocy max 180W i sprawności min 90% - konstrukcja pozwalająca na beznarzędziowy dostęp do komponentów (pamięci, dysków, napędów) - minimalna ilość wnęk. 1x 5,25” zewnętrzne, 1x 3,5” wewnętrzne - możliwość zamontowania 1 dysku 3,5” lub do 2 dysków 2,5” - wizualny system diagnostyczny do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizujący co najmniej: <ul style="list-style-type: none"> - awarie procesora - uszkodzenie grafiki - uszkodzenie zasilacza - Głośność jednostki centralnej mierzoną zgodnie z normą ISO 7779 lub równoważną oraz wykazaną zgodnie z normą ISO 9296 lub równoważną z pozycji operatora w trybie jałowym (IDLE) wynoszącą maksymalnie 23 dB (załączyć oświadczenie wykonawcy lub raport z przeprowadzonych badań głośności)
Oprogramowanie	<ul style="list-style-type: none"> - System operacyjny spełniający następujące wymagania poprzez wbudowane mechanizmy, bez konieczności użycia dodatkowych aplikacji: <ul style="list-style-type: none"> • Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek;

	<ul style="list-style-type: none"> • Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu; • Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW; • Internetowa aktualizacja zapewniona w języku polskim; • Wbudowana zaporę internetową (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; • Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimedialny, pomoc, komunikaty systemowe; • Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi) • Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer • Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służąca do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta. • Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. • Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. • Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych. • Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika. • Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. • Wbudowany system pomocy w języku polskim; • Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); • Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; • Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509; • Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji; • System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; • Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach; • Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń; • Graficzne środowisko instalacji i konfiguracji; • Transakcyjny system plików pozwalający na stosowanie przydziałów na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe; • Zarządzanie kontami użytkowników sieci oraz urządzeniami
--	---

	<p>sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe</p> <ul style="list-style-type: none"> • Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej; • Możliwość przywracania plików systemowych; • System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.) • Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np przy użyciu numerów identyfikacyjnych sprzętu). • Telefoniczne wsparcie techniczne w języku polskim w dni robocze od 8:00 do 17:00 zapewniony przez producenta lub dostawcę co najmniej przez 5 lat od chwili zakupu <p>- Oprogramowanie szyfrujące zawartość twardego dysku zgodnie z certyfikatem X.509 oraz algorytmem szyfrującym AES 128 bit oraz AES 256bit, współpracujące z wbudowaną sprzętową platformą bezpieczeństwa</p> <p>- Pakiet biurowy spełniający wymagania techniczne określone w pkt. 6.6</p> <p>- Pakiet antywirusowy zapewniający w okresie realizacji projektu dostęp do najnowszych baz szczepionek wirusów, oraz wsparcie techniczne producenta w języku polskim spełniający wymagania techniczne określone w pkt. 6.7</p>
Bezpieczeństwo	<p>Komputer musi posiadać:</p> <ul style="list-style-type: none"> - zintegrowany dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania (zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego) - zintegrowany fabrycznie w obudowie czujnik otwarcia obudowy - możliwość zastosowania zabezpieczenia fizycznego w postaci linki metalowej lub kłódki - wbudowaną technologię zarządzania i monitorowania na poziomie sprzętowym działającą niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, posiadającą sprzętowe wsparcie technologii wirtualizacji, wbudowany sprzętowy firewall, zarządzany i konfigurowany z serwera zarządzania oraz niedostępny dla lokalnego systemu OS i lokalnych aplikacji, a także umożliwiającą: <ul style="list-style-type: none"> - monitorowanie konfiguracji komponentów komputera - CPU, pamięć, HDD, wersje BIOS; - zdalną konfigurację ustawień BIOS; - zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego; <ul style="list-style-type: none"> - zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nieulotnej; - technologia zarządzania i monitorowania komputerem na poziomie sprzętowym powinna być zgodna z otwartymi standardami DMTF WS-MAN 1.0.0 (http://www.dmtf.org/standards/wsman) oraz DASH 1.0.0 (http://www.dmtf.org/standards/mgmt/dash/); - nawiązywanie przez sprzętowy mechanizm zarządzania zdalnego szyfrowanego protokołem SSL/TLS połączenia z predefiniowanym serwerem zarządzającym, w definiowanych

		odstępach czasu, w przypadku wystąpienia predefiniowanego zdarzenia lub błędu systemowego oraz na żądanie użytkownika z poziomu BIOS; - wbudowany sprzętowo log operacji zdalnego zarządzania, możliwy do kasowania tylko przez upoważnionego użytkownika systemu sprzętowego zarządzania zdalnego.
Wymagania dodatkowe		Zintegrowane w obudowie: - porty USB: min. 6 gniazd, w tym co najmniej 4 w standardzie USB 3.0 - złącza video: : min. 1x DisplayPort - porty audio: z przodu/boku obudowy - gniazdo Gigabit Ethernet z obsługą PXE, WoL, ASF 2.0, ACPI, - karta WLAN 802.11agn, Bluetooth, 2x PS/2, głośnik, dwa mikrofony, kamera min. 2 MPix HD Zintegrowane na płycie głównej min. 1 złącze mSATA Klawiatura w układzie polski programisty, mysz optyczna z dwoma klawiszami oraz rolką (scroll)
Certyfikaty standardy	i	- ISO9001 lub równoważny dla producenta sprzętu, - EnergyStar 5.0 - Deklaracja zgodności CE
Wsparcie techniczne		- Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta , jego przedstawiciela lub wykonawcy. - Dostęp do najnowszych sterowników i uaktualnień realizowany poprzez podanie na dedykowanej stronie internetowej numeru seryjnego lub modelu komputera
Gwarancja		
Zestaw wyposażeniem dodatkowym	z	3 lata gwarancji świadczonej w miejscu eksploatacji sprzętu - czas reakcji serwisu: do końca następnego dnia roboczego - telefoniczne wsparcie techniczne dla użytkowników: dni robocze w godzinach 8 ⁰⁰ -20 ⁰⁰ - w przypadku awarii komputerowych dysków twardych - dysk uszkodzony pozostaje u Zamawiającego

6. Dostawa oraz modernizacja sprzętu komputerowego do uczestników projektu

Wykonawca jest zobowiązany do skalkulowania wszelkich kosztów związanych z:

- zakupem sprzętu komputerowego i oprogramowania (licencje na oprogramowanie powinny zapewnić Zamawiającemu możliwość wielokrotnego wypożyczenia lub użyczenia sprzętu komputerowego wraz z oprogramowaniem jednostkom podległym, o ile jest to wymagane przez producentów oprogramowania),
- dostawą i instalacją sprzętu w docelowym miejscu eksploatacji (w Jednostkach Podległych oraz u Uczestników końcowych projektu).
- podłączeniem i uruchomieniem dostępu do sieci Internet dla dostarczonych urządzeń, w ramach wybudowanej infrastruktury
- oznakowaniem przedmiotu zamówienia zgodnie z wytycznymi Władzy Wdrażającej zawartymi w „Przewodniku w zakresie promocji projektów finansowanych w ramach Programu Operacyjnego Innowacyjna Gospodarka, 2007- 2013”
- świadczeniem usług gwarancyjnych i serwisowych dla dostarczonych urządzeń na warunkach określonych w SIWZ
- świadczeniem wsparcia technicznego dla dostarczonego sprzętu komputerowego i oprogramowania i w dni robocze w godzinach 8⁰⁰-20⁰⁰.
- przeprowadzeniem jednorazowej modernizacji sprzętu komputerowego w ostatnim kwartale realizacji projektu, obejmującej wymianę zużytych podzespołów, w szczególności klawiatur i myszy i konserwację oprogramowania.

6.1 Zestaw Komputerowy z drukarką z przeznaczeniem dla gospodarstw domowych– (200 szt.)

Komputer stacjonarny przeznaczony do zapewnienia beneficjentom ostatecznym projektu dostępu do sieci Internet, dedykowany do obsługi aplikacji biurowych, grafiki prezentacyjnej i multimediów	
Nazwa atrybutu	Wymagane minimalne
Wydajność	Procesor dedykowany do pracy w komputerach stacjonarnych, uzyskujący w teście Passmark CPU Mark wynik min. 3000 punktów. Wydruk ze strony internetowej http://www.cpubenchmark.net dla oferowanego procesora (nie starszy niż na dzień 01.09.2014r.) należy dołączyć do oferty Komputer w oferowanej przez Wykonawcę konfiguracji testowany przy rozdzielczości ekranu min. 1920 x 1080 powinien osiągać w teście wydajności SYSMark2012 System Management wynik co najmniej 130 pkt. (szczegółowy raport z przeprowadzonych testów należy dołączyć do oferty).
Pamięć	min. 4GB pamięci operacyjnej (możliwość rozbudowy do 16GB) min. 500GB pamięci masowej SATA
Grafika	Komputer w oferowanej przez Wykonawcę konfiguracji testowany przy rozdzielczości ekranu min. 1920 x 1080 powinien osiągać w teście wydajności SYSMark2012 3D Modeling wynik co najmniej 125 pkt. (szczegółowy raport z przeprowadzonych testów należy dołączyć do oferty).
Napędy wbudowane	Nagrywarka DVD +/-RW wraz z oprogramowaniem do nagrywania i odtwarzania płyt Czytnik kart multimedialnych
Funkcjonalność BIOS	Możliwość: - weryfikacji numeru seryjnego komputera - skonfigurowania hasła „Power On” oraz ustawienia hasła dostępu do BIOSu (administratora) w sposób gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS, - ustawienia hasła na dysku - blokady/wyłączenia portów USB, COM, karty sieciowej, karty audio; - blokady/wyłączenia kart rozszerzeń/slotów PCI - kontroli sekwencji boot-owania; - startu systemu z urządzenia USB - blokowania boot-owania stacji roboczej z zewnętrznych urządzeń - ustawienia hasła na poziomie administratora bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych - automatycznej (lub na żądanie) aktualizacji BIOS przez sieć włączaną z poziomu BIOS przez użytkownika, bez konieczności uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.
Funkcjonalność obudowy	-obudowa małogabarytowa z możliwością pracy w pionie i poziomie - konstrukcja pozwalająca na beznarzędziowy dostęp do komponentów (kart rozszerzeń, napędów) - minimalna ilość wnęk. 1x 5,25” zewnętrzne, 1x 3,5” zewnętrzne, 1x 3,5” wewnętrzne, 1x 2,5” wewnętrzne - zasilacz o mocy max. 250W i skuteczności min. 90% - wizualny system diagnostyczny do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizujący co najmniej: - awarie procesora - uszkodzenie grafiki - uszkodzenie zasilacza - Głośność jednostki centralnej mierzoną zgodnie z normą ISO 7779 lub równoważną, oraz wykazaną zgodnie z normą ISO 9296 lub równoważną z pozycji operatora w trybie jałowym (IDLE) wynoszącą maksymalnie 26 dB (załączyć oświadczenie wykonawcy lub raport z przeprowadzonych badań głośności)
Oprogramowanie	- System operacyjny spełniający następujące wymagania poprzez wbudowane mechanizmy, bez konieczności użycia dodatkowych aplikacji:

	<ul style="list-style-type: none"> • Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek; • Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu; • Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW; • Internetowa aktualizacja zapewniona w języku polskim; • Wbudowana zaporę internetową (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; • Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimedialny, pomoc, komunikaty systemowe; • Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi) • Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer • Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służąca do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta. • Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. • Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. • Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych. • Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika. • Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. • Wbudowany system pomocy w języku polskim; • Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); • Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; • Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509; • Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji; • System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; • Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach; • Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń; • Graficzne środowisko instalacji i konfiguracji; • Transakcyjny system plików pozwalający na stosowanie przydziałów na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe; • Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi
--	--

	<p>katalogowe</p> <ul style="list-style-type: none"> • Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej; • Możliwość przywracania plików systemowych; • System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.) • Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np przy użyciu numerów identyfikacyjnych sprzętu). • Telefoniczne wsparcie techniczne w języku polskim w dni robocze od 8:00 do 17:00 zapewniony przez producenta lub wykonawcę co najmniej przez 3 lata od chwili zakupu <p>- Pakiet biurowy spełniający wymagania techniczne określone w pkt. 6.6 - Pakiet antywirusowy zapewniający w okresie realizacji projektu dostęp do najnowszych baz szczepionek wirusów, oraz wsparcie techniczne producenta w języku polskim</p>
Bezpieczeństwo	<p>Komputer musi posiadać:</p> <ul style="list-style-type: none"> - zintegrowany dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania (zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego) - zintegrowany fabrycznie w obudowie czujnik otwarcia obudowy - możliwość zastosowania zabezpieczenia fizycznego w postaci linki metalowej i kłódki - wbudowaną technologię zarządzania i monitorowania na poziomie sprzętowym działającą niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, posiadającą sprzętowe wsparcie technologii wirtualizacji, wbudowany sprzętowy firewall, zarządzany i konfigurowany z serwera zarządzania oraz niedostępny dla lokalnego systemu OS i lokalnych aplikacji, a także umożliwiającą: <ul style="list-style-type: none"> - monitorowanie konfiguracji komponentów komputera - CPU, pamięć, HDD, wersje BIOS płyty głównej; - zdalną konfigurację ustawień BIOS; - zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego; - zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nieulotnej; - technologia zarządzania i monitorowania komputerem na poziomie sprzętowym powinna być zgodna z otwartymi standardami DMTF WS-MAN 1.0.0 (http://www.dmtf.org/standards/wsman) oraz DASH 1.0.0 (http://www.dmtf.org/standards/mgmt/dash/); - nawiązywanie przez sprzętowy mechanizm zarządzania zdalnego szyfrowanego protokołem SSL/TLS połączenia z predefiniowanym serwerem zarządzającym, w definiowanych odstępach czasu, w przypadku wystąpienia predefiniowanego zdarzenia lub błędu systemowego oraz na żądanie użytkownika z poziomu BIOS; - wbudowany sprzętowo log operacji zdalnego zarządzania, możliwy do kasowania tylko przez upoważnionego użytkownika systemu sprzętowego zarządzania zdalnego.
Wymagania dodatkowe	<p>Zintegrowane w obudowie:</p> <ul style="list-style-type: none"> - porty USB: min. 10 gniazd, w tym co najmniej 4 w standardzie USB 3.0 - złącza video: : min. D-Sub, DisplayPort - porty audio: z przodu i z tyłu obudowy

		<ul style="list-style-type: none"> - gniazdo Gigabit Ethernet z obsługą PXE, WoL, ASF 2.0, ACPI, - RS232, 2x PS/2, głośnik <p>Zintegrowane na płycie głównej: min. 3 złącza PCI Express x1, 1 złącze PCI Express x16 Klawiatura w układzie polski programisty, mysz optyczna z dwoma klawiszami oraz rolką (scroll)</p>
Certyfikaty standardy	i	<ul style="list-style-type: none"> - Certyfikat ISO9001 lub równoważny producenta sprzętu - EnergyStar 5.0 - Deklaracja zgodności CE
Wsparcie techniczne		<ul style="list-style-type: none"> - Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela lub wykonawcy. - Dostęp do najnowszych sterowników i uaktualnień realizowany poprzez podanie na dedykowanej stronie internetowej producenta, jego przedstawiciela lub wykonawcy numeru seryjnego lub modelu komputera
Monitor		
Typ ekranu		Ekran ciekłokrystaliczny z aktywną matrycą TFT 21"
Czas reakcji matrycy		max 5ms
Rozdzielczość		min. 1920 x 1080 przy 60Hz
Dostępna regulacja		min. kąt nachylenia ekranu
Podświetlenie		LED
Współczynnik kontrastu		min. 600:1
Zużycie energii		22W (typowe); 0,3W (czuwanie)
Złącze		zgodne ze złączem video jednostki centralnej
Certyfikaty standardy	i	<ul style="list-style-type: none"> - Certyfikat ISO9001 lub równoważny dla producenta sprzętu - EnergyStar 5.0 - Deklaracja zgodności CE
Wyposażenie dodatkowe		
Drukarka (Typ A)		<ul style="list-style-type: none"> - Obsługiwane funkcje: drukowanie, kopiowanie, skanowanie - Parametry drukowania: druk w kolorze z prędkością do 10str/min, druk w czerni z prędkością do 25str./min., rozdzielczość druku do: 6000x1200 dpi - Parametry kopiowania: rozdzielczość kopii do: 1200x1200 dpi - Parametry skanowania: rozdzielczość skanowania do: 1200x2400 dpi, format plików wynikowych: jpeg, tif, pdf, bmp, png - Obsługa papieru: podajnik min. 100 ark, odbiornik min. 50 ark. - Interfejs komunikacyjny: USB, WiFi - Inne cechy: wyświetlacz LCD, pamięć RAM 64MB -EnergyStar, - Deklaracja zgodności CE - wyposażenie: startowy zestaw materiałów eksploatacyjnych, kabel sygnałowy i zasilający
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: 25ns, bezpiecznik nadprądowy, możliwość montażu na ścianie
Gwarancja		
Zestaw wyposażeniem dodatkowym	z	<ul style="list-style-type: none"> 3 lata gwarancji świadczonej w miejscu eksploatacji sprzętu - czas reakcji serwisu: do końca następnego dnia roboczego - telefoniczne wsparcie techniczne dla użytkowników: dni robocze w godzinach 8⁰⁰-20⁰⁰ - w przypadku awarii komputerowych dysków twardych - dysk uszkodzony pozostaje u Zamawiającego

6.2 Zestaw Komputerowy z przeznaczeniem dla jednostek podległych – (66szt.)

Komputer stacjonarny typu All-in-One przeznaczony do zapewnienia jednostkom podległym beneficjentowi dostępu do sieci Internet, dedykowany do obsługi aplikacji biurowych, poczty elektronicznej, grafiki prezentacyjnej, multimediiów i nauczania na odległość	
Nazwa atrybutu	Wymagane minimalne
Wydajność	Procesor dedykowany do pracy w komputerach stacjonarnych, uzyskujący w teście Passmark CPU Mark wynik min. 4000 punktów. Wydruk ze strony internetowej http://www.cpubenchmark.net dla oferowanego procesora (nie starszy niż na dzień 01.09.2014r.) należy dołączyć do oferty
Pamięć	min. 4GB pamięci operacyjnej (możliwość rozbudowy do 16GB) min. 500GB pamięci masowej SATA
Grafika	Uzyskująca w teście wydajności Average G3D Mark wynik min. 600 punktów. Wydruk ze strony internetowej http://www.videobenchmark.net dla oferowanej (nie starszy niż na dzień 01.09.2014r.) należy dołączyć do oferty
Napędy wbudowane	Nagrywarka DVD +/-RW wraz z oprogramowaniem do nagrywania i odtwarzania płyt Czytnik kart multimedialnych
Funkcjonalność BIOS	- możliwość weryfikacji w BIOS numeru seryjnego komputera, - możliwość weryfikacji konfiguracji sprzętowej (model komputera, procesor, pamięć, dysk, napęd optyczny) - możliwość selektywnego (pojedynczego) blokowania portów USB z poziomu BIOS - możliwość bootowania systemu z czytnika kart - możliwość ustawienia portów USB, sieci, napędu DVD w tryb „no-boot” - możliwość wyłączenia kamery wbudowanej, czytnika karty, - możliwość blokowania lub wyłączenia przycisków na przedniej obudowie,
Funkcjonalność obudowy	- typ All-in-One (komputer zintegrowany w obudowie wraz z monitorem) z ekranem LED min. 20” HD+ (1600x900) o kontraście typowym min.: 1000:1; czasie reakcji matrycy do 5ms, jasności min.: 250 cd/m2, kątach widzenia min. 160/170 stopni (w pionie i poziomie) - dostępna regulacja w pionie (min. 100mm), kąta nachylenia ekranu (-10/+25 stopni), obrotowa podstawa (-45/+45 stopni), - zasilacz wewnętrzny o mocy max 150W i sprawności min 85% - głośność jednostki centralnej mierzoną zgodnie z normą ISO 7779 lub równoważną, oraz wykazaną zgodnie z normą ISO 9296 lub równoważną w pozycji operatora w trybie jałowym (IDLE) wynoszącą maksymalnie 23 dB(załączyć oświadczenie wykonawcy, lub raport z przeprowadzonych badań głośności)
Oprogramowanie	- System operacyjny spełniający następujące wymagania poprzez wbudowane mechanizmy, bez konieczności użycia dodatkowych aplikacji: <ul style="list-style-type: none"> • Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek; • Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu; • Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW; • Internetowa aktualizacja zapewniona w języku polskim; • Wbudowana zaporę internetową (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; • Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediiów, pomoc, komunikaty systemowe; • Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi) • Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer • Interfejs użytkownika działający w trybie graficznym z elementami

3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służąca do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta.

- Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
- Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych.
- Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych.
- Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika.
- Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
- Wbudowany system pomocy w języku polskim;
- Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
- Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
- Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;
- Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji;
- System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
- Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach;
- Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń;
- Graficzne środowisko instalacji i konfiguracji;
- Transakcyjny system plików pozwalający na stosowanie przydziałów na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe;
- Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe
- Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej;
- Możliwość przywracania plików systemowych;
- System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.)
- Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).
- Telefoniczne wsparcie techniczne w języku polskim w dni robocze od 8:00 do 17:00 zapewniony przez producenta lub wykonawcę co najmniej przez 3 lata od chwili zakupu

- Pakiet biurowy spełniający wymagania techniczne określone w pkt. 6.6
- Pakiet antywirusowy zapewniający w okresie realizacji projektu dostęp do najnowszych baz szczepionek wirusów, oraz wsparcie techniczne

	producenta w języku polskim spełniający wymagania techniczne określone w pkt. 6.7
Bezpieczeństwo	Komputer musi posiadać: - zintegrowany dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania (zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego) - zintegrowany fabrycznie w obudowie czujnik otwarcia obudowy - możliwość zastosowania zabezpieczenia fizycznego w postaci linki metalowej lub kłódki
Wymagania dodatkowe	Zintegrowane w obudowie: - porty USB: min. 6 gniazd, w tym co najmniej 2 w standardzie USB 3.0 - porty audio: z przodu/boku obudowy - złącza: D-Sub, RS-232, PS/2 - gniazdo Gigabit Ethernet, karta WLAN 802.11agn, - głośniki stereo (2x2W) - kamera min. 1 MPixHD z mechanicznąprzesłoną obiektywu Klawiatura w układzie polski programisty, mysz optyczna z dwoma klawiszami oraz rolką (scroll)
Certyfikaty i standardy	- Certyfikat ISO9001 lub równoważny dla producenta sprzętu - EnergyStar 5.0 - Deklaracja zgodności CE
Wsparcie techniczne	- Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela lub wykonawcy. - Dostęp do najnowszych sterowników i uaktualnień realizowany poprzez podanie na dedykowanej stronie internetowej producenta , jego przedstawiciela lub wykonawcy numeru seryjnego lub modelu komputera
Wyposażenie dodatkowe	
Słuchawki z mikrofonem	Wbudowany regulator dźwięku, miseczki słuchawek wykonane z pianki, mikrofon z redukcją hałasu, obrotowym wysięgnikiem i możliwością umiejscowienia po lewej i prawej stronie, typ złącza: 2x 3.5mm
Gwarancja	
Zestaw wraz z wyposażeniem dodatkowym	3 lata gwarancji świadczonej w miejscu eksploatacji sprzętu - czas reakcji serwisu: do końca następnego dnia roboczego - telefoniczne wsparcie techniczne dla użytkowników: dni robocze w godzinach 8 ⁰⁰ -20 ⁰⁰ - w przypadku awarii komputerowych dysków twardych - dysk uszkodzony pozostaje u Zamawiającego

6.3 Drukarka atramentowa kolor z przeznaczeniem dla Jednostek Podległych – 5 szt.

Drukarka (Typ B)	
Nazwa atrybutu	Wymagane minimalne
Funkcja	4w1 - drukowanie, kopiowanie, skanowanie, faksowanie
Szybkość druku	w czerni i kolorze: 20 str. /min
Szybkość kopiowania	w czerni i kolorze: 20 str. /min
Rozdzielczość druku	w czerni i kolorze: do 1200 x 1200 dpi
Rozdzielczość skanowania	1200 x 1200 dpi
Pojemność podajnika	100 arkuszy dla druku, 20 arkuszy dla kopiowania/skanowania
Pojemność odbiornika	100 arkuszy dla druku, 20 arkuszy dla kopiowania/skanowania
Interfejsy standardowe	USB 2.0, WiFi 802.11b/g/n, czytnik kart pamięci
Pamięć urządzenia	64 MB

Systemy operacyjne	Kompatybilność z oferowanym systemem operacyjnym
Certyfikaty i standardy	- EnergyStar - Deklaracja zgodności CE
Gwarancja	3 lata gwarancji świadczonej w miejscu eksploatacji sprzętu

6.4 Drukarka laserowa mono z przeznaczeniem dla Jednostek Podległych – 8 szt.

Drukarka (Typ C)	
Nazwa atrybutu	Wymagane minimalne
Szybkość druku	w czerni: 25 str. / min.
Rozdzielczość druku	w czerni: do 600 x 600 dpi
Pojemność podajnika	250 arkuszy
Pojemność odbiornika	150 arkuszy
Interfejsy standardowe	USB 2.0, Ethernet 10/100TX
Pamięć urządzenia	32 MB
Systemy operacyjne	Kompatybilność z oferowanym systemem operacyjnym
Certyfikaty i standardy	- EnergyStar - Deklaracja zgodności CE
Gwarancja	3 lata gwarancji świadczonej w miejscu eksploatacji sprzętu

6.5 Drukarka laserowa kolorowa z przeznaczenie dla Jednostek Podległych – 2 szt.

Drukarka (Typ D)	
Nazwa atrybutu	Wymagane minimalne
Szybkość druku	w czerni i kolorze: 14 str. /min
Rozdzielczość druku	w czerni i kolorze: do 600 x 600 dpi
Pojemność podajnika	150 arkuszy
Pojemność odbiornika	100 arkuszy
Interfejsy standardowe	USB 2.0, Ethernet 10/100TX
Pamięć urządzenia	64 MB
Systemy operacyjne	Kompatybilność z oferowanym systemem operacyjnym
Certyfikaty i standardy	- EnergyStar - Deklaracja zgodności CE
Gwarancja	3 lata gwarancji świadczonej w miejscu eksploatacji sprzętu

6.6 Pakiet biurowy

Nazwa atrybutu	Wymagania minimalne
Interfejs użytkownika	- polska wersja językowa interfejsu użytkownika - interaktywna pomoc w języku polskim - biuletyny techniczne i pomoc techniczna producenta oprogramowania świadczone w języku polskim
Tworzenie i edycja dokumentów	Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: - posiada kompletny i publicznie dostępny opis formatu, - ma zdefiniowany układ informacji w postaci XML - umożliwia wykorzystanie schematów XML - wspiera podpis elektroniczny
Zawartość pakietu	- edytor tekstów - arkusz kalkulacyjny

	- narzędzie do przygotowywania i prowadzenia prezentacji - program do tworzenia i zarządzania bazami danych Wszystkie elementy składowe pakietu muszą pochodzić od jednego producenta
--	---

6.7 Oprogramowanie antywirusowe oraz antyspyware, wraz z konsolą do zdalnej administracji

Wymagania minimalne względem oprogramowania antywirusowego

Pełne wsparcie dla systemów operacyjnych oferowanych przez Wykonawcę w komputerach stacjonarnych i przenośnych (w wersji 32 i 64-bit)

Wersja programu, pomoc (help) i dokumentacja dostępna w języku polskim

Ochrona antywirusowa i antyspyware

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
3. Wbudowana technologia do ochrony przed rootkitami.
4. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
5. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
6. System 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.
7. 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).
8. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
9. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
10. Możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Skanowanie plików spakowanych i skompresowanych.
12. Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (w tym z uwzględnieniem plików bez rozszerzeń).
13. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
14. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
15. 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.
16. 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).
17. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
18. Możliwość definiowania różnych portów dla POP3, na których ma odbywać się skanowanie.
19. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
20. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
21. 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.
22. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
23. Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie.
24. 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.

25. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.
26. Aktualizacje modułów analizy heurystycznej.
27. 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.
28. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
29. Wysyłanie zagrożeń do laboratorium powinno być możliwe z serwera zdalnego zarządzania i lokalnie z każdej stacji roboczej w przypadku komputerów mobilnych.
30. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń powinny być w pełni anonimowe.
31. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
32. Możliwość automatycznego wysyłania powiadomienia o wykrytych zagrożeniach do dowolnej stacji roboczej w sieci lokalnej.
33. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.
34. Interfejs programu powinien oferować funkcję pracy w trybie bez grafiki gdzie cały interfejs wyświetlany jest w formie formatek i tekstu.
35. Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS i POP3S.
36. Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
37. Administrator powinien mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
38. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.
39. 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.
40. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji powinno być takie samo.
41. Program powinien mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiegś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.
42. 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.
43. 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.
44. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB powinien umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
45. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB powinien pracować w trybie graficznym.
46. Program powinien być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.
47. 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.
48. 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.
49. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.

50. 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).
51. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
52. 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).
53. Do każdego zadania aktualizacji można przypisać dwa różne profile z innym ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja).
54. 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 rezerwowo pobierający aktualizację z Internetu.
55. Program wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
56. Praca programu musi być niezauważalna dla użytkownika.
57. Program powinien posiadać dwie wersje interfejsu (standardowy – z ukrytą częścią ustawień oraz zaawansowany – z widocznymi wszystkimi opcjami)
58. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania.

7. Usługi administrowania i serwisowania systemu (sieci szerokopasmowej oraz sprzętu komputerowego), w tym kontrola ewentualnych nadużyć w okresie realizacji projektu (Operator Infrastruktury).

7.1 Serwis i utrzymywanie sprzętu komputerowego w Jednostkach Podległych w ramach zadań koordynacyjnych (66 zestawy komputerowych z dostępem do Internetu)

Wykonawca (Operator Infrastruktury) zobowiązany jest do instalacji 66 szt. sprzętu komputerowego (zestawów komputerowych, peryferyjnych oraz urządzeń umożliwiających korzystanie z usługi dostępu do Internetu) w lokalizacji Jednostek Podległych objętej projektem.

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

- świadczenia usług serwisu sprzętu komputerowego i urządzeń internetowych w miejscu instalacji
- kontrola i bieżące serwisowanie wydanych zestawów komputerowych w zakresie sprzętu i oprogramowania
- świadczenia usług wsparcia technicznego dla jednostek poprzez określenie wydzielonego nr telefonu serwisowego
- podjęcia działań serwisowych w ciągu maksymalnie 4 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
- dokonywania przeglądów okresowych sprzętu, co najmniej jednego przeglądu w roku obejmującego diagnostykę oraz konserwację sprzętu

7.2 Serwis i utrzymywanie sprzętu komputerowego w gospodarstwach domowych (200 zestawów komputerowych z dostępem do Internetu)

Wykonawca (Operator Infrastruktury) zobowiązany jest do przekazania (protokolarnie) i instalacji 200 szt. zestawów komputerowych , w tym także urządzeń peryferyjnych i urządzeń umożliwiających korzystanie z usługi dostępu do Internetu) użytkownikom końcowym, określonym 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:

- instalacji i konfiguracji urządzeń odbiorczych do Internetu
- protokolarnego przekazania sprzętu komputerowego
- kontrola i bieżące serwisowanie zestawów komputerowych w zakresie sprzętu i oprogramowania
- 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

Uwaga!

Wykonawca (Operator Infrastruktury) odpowiedzialny jest za odzyskanie sprzętu w razie nieprawidłowego użytkowania przez beneficjentów końcowych.

7.3 Serwis i utrzymanie infrastruktury sieci szerokopasmowej

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

- bieżące monitorowanie infrastruktury i wykrywanie awarii
- bieżące usuwanie awarii w ciągu maksymalnie 8 godzin – dotyczy urządzeń aktywnych stanowiących wyposażenie Centrum Zarządzania siecią
- bieżące usuwanie awarii w ciągu maksymalnie 48 godzin – pozostałe elementy infrastruktury
- bieżące usuwanie awarii elementów i urządzeń sieci, zainstalowanych w beneficjentów końcowych (200 gospodarstw domowych i 14 Jednostkach Podległych)
- 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, (punktów dostępowych WiFi oraz innych urządzeń)
- prowadzenie elektronicznej ewidencji zgłoszeń serwisowych

8. Zapewnienie usługi dostępu do Internetu dla 200 gospodarstw domowych oraz 66komputerów w Jednostkach Podległych przez okres realizacji projektu.

8.1 Dostawa, montaż i konfiguracja urządzeń dostępowych, przyłączenie do sieci 200 gospodarstw domowych

Wymagana jest dostawa urządzeń, (lub zestawu urządzeń) zapewniających podłączenie komputera do Internetu dla 200 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

- a) Wykonawca dostarczy wszelkie urządzenia potrzebne do skonfigurowania połączeń: urządzenia dostępne, okablowanie oraz jeśli to będzie wymagane maszty i elementy mocowania anten
- b) urządzenia dostępne muszą spełniać wymagania określonej w punkcie 4.5 lub 4.6
- c) Zamawiający wyklucza rozwiązania oparte na kartach rozszerzeń montowanych wewnątrzobudowy komputera
- d) Wykonawca będzie zobowiązany do konfiguracji, utrzymania i serwisowania dostarczonych i zainstalowanych urządzeń przez okres realizacji projektu, 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
- e) Wszystkie urządzenia powinny posiadać 36 miesięczną gwarancję

8.2 Usługa dostępu do Internetu

Zamawiający wymaga świadczenia usług dostępu do Internetu dla 200 gospodarstw domowych oraz 14 jednostek podległych Gminy, przez okres realizacji projektu określony w SIWZ.

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 100Mb/s FDx(symetryczne)
- brak limitu transferu danych
- brak limitów i ograniczeń czasowych korzystania z usługi
- zapewnienie puli zewnętrznych adresów IP w minimalnej ilości 16 (w ramach jednej klasy)

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

9. Szkolenia z zakresu obsługi komputera (systemu operacyjnego, pakietu biurowego oraz Internetu) – 200 osób

9.1 Wstęp

Przedmiotem zadania jest przeszkolenie co najmniej 200 osób (Beneficjentów ostateczny projektu pn. „Przeciwdziałanie wykluczeniu cyfrowemu w Gminie Poraj” realizowanego w ramach działania POIG 8.3. Celem tych szkoleń jest nabycie podstawowej wiedzy z zakresu obsługi komputera, obsługi oprogramowania biurowego, oraz obsługi uruchomionego łącza internetowego oraz aplikacji internetowych w ramach projektu. Beneficjenci, dzięki tym szkoleniom powinni nabyć wiedzę pozwalającą im na samodzielne korzystanie z sprzętu komputerowego, oraz wykonywanie podstawowych zadań związanych z tworzeniem, edycją dokumentów za pomocą oprogramowania biurowego oraz korzystania z zasobów Internetu.

Wykonawca jest zobowiązany ramach w/w zadania do przeszkolenia co najmniej 200 osób łącznie przy czym :

- a) minimalna liczba grup szkoleniowych – 20
- b) maksymalna liczba osób w grupie szkoleniowej – 10
- c) minimalna liczba godzin szkoleniowych na grupę – 10
- d) z każdego gospodarstwa domowego może brać udział min.1 osoba
- e) minimalna liczba dni szkoleniowych - 2

9.2 Wymagania ogólne stawiane Wykonawcy w zakresie szkoleń

1. Wykonawca przed rozpoczęciem szkolenia oznaczy pomieszczenia, materiały szkoleniowe, dokumentację szkoleniową i środki techniczne zgodnie z Wytocznymi dotyczącymi oznaczania projektów w ramach Programu Operacyjnego Innowacyjna Gospodarka ustalone z Zamawiającym.

2. W ciągu 7 dni od podpisania umowy, Wykonawca wyznaczy koordynatora szkoleń. Koordynator szkoleń będzie przekazywał dokumentację, wszystkie informacje na temat szkoleń i inne niezbędne. Będzie to osoba do bieżących kontaktów roboczych, za pośrednictwem której Zamawiający będzie się kontaktował z Wykonawcą w zakresie szkoleń.

3. W ciągu 7 dni od podpisania umowy Zamawiający przekaze Wykonawcy listę osób z adresami zakwalifikowanych do szkolenia oraz informację o ewent. osobach niepełnosprawnych, z podaniem stopnia niepełnosprawności.

4. W ciągu 14 dni od podpisania umowy, Wykonawca przekaże Zamawiającemu szczegółowy harmonogram szkoleń wraz z programem uwzględniający czas szkolenia w poszczególne dni tygodnia, ilość grup szkoleniowych w danym dniu, tematykę szkoleń z podziałem na poszczególne dni, salę szkoleniową. Po akceptacji przez Zamawiającego lub wprowadzeniu stosownych zmian Wykonawca będzie mógł przystąpić do szkoleń.

5. Wykonawca we własnym zakresie będzie informował wszystkich uczestników szkoleń o terminach , miejscu szkolenia lub zmianach w tym zakresie .

6. Wykonawca zobowiązany jest do prowadzenia pełnej dokumentacji związanej ze szkoleniem, osobnej dla każdej grupy szkoleniowej, tj:

- listy obecności,
- dziennika zajęć,
- dokumentacji zdjęciowej,
- list z pokwitowaniem odbioru materiałów szkoleniowych,
- ankiet przed i po szkoleniu, określającym poziom nabytej wiedzy,
- zdjęcia obrazujące udział uczestników w szkoleniu – na płycie CD – co najmniej 2 zdjęcia z każdego szkolenia dla każdej grupy, gdzie kadry zdjęcia obejmują wszystkich uczestników,

7. Wykonawca zobowiązany jest w ciągu 7 dni od zakończenia wszystkich szkoleń do przekazania Zamawiającemu materiałów wg. pkt. 6 dla danej grupy szkoleniowej wraz z jednym kompletem materiałów szkoleniowych w wersji drukowanej oraz elektronicznej.

8. Wykonawca zobowiązany jest do wystawienia uczestnikom szkolenia certyfikatów ukończenia szkolenia. Warunkiem otrzymania certyfikatu jest udział wytypowanego uczestnika w zajęciach szkoleniowych zgodnie z przyjętą metodologią szkolenia.

9. Szkolenia odbędą się na sprzęcie komputerowym dostarczonym przez Wykonawcę.

10. Wykonawca musi dysponować własnymi pomocami dydaktycznymi, w tym co najmniej projektorem multimedialnym, ekran, tablice, plansze itp
11. Wykonawca w ramach realizacji przedmiotu zamówienia musi zapewnić na własny koszt pomieszczenia oraz łącze do Internetu niezbędne do prowadzenia zajęć.
12. Wykonawca zapewni pomieszczenie szkoleniowe na terenie gminy Poraj. W przypadku lokalizacji poza gminą Poraj Wykonawca musi zapewnić na własny koszt transport BO do miejsca szkolenia .
13. Wykonawca zobowiązany jest do indywidualizacji kształcenia poprzez prowadzenie systematycznej oceny postępów w nauce osiąganym przez poszczególnych jego uczestników/uczestniczek oraz zwiększenia pomocy uczestnikom/uczestniczkom mającym problemy podczas szkolenia.
14. Wykonawca zobowiązany jest pod rygorem odmowy przez Zamawiającego zapłaty za kurs danych osób, do bieżącego informowania Zamawiającego o:
 - nieobecności na szkoleniu osób na nie skierowanych (imię i nazwisko osoby),
 - rezygnacji z uczestnictwa w szkoleniu w trakcie jego trwania przez osoby na nie skierowaneO w/w sytuacjach Wykonawca jest zobowiązany informować Zamawiającego oraz Inżyniera Projektu (tel , list, fax lub drogę mailową za zwrotnym potwierdzeniem) w ciągu 3 dni od wystąpienia takiej sytuacji
15. W celu zapewnienia wysokiej jakości poziomu szkolenia, Wykonawca powinien dysponować min. 2 wykwalifikowanymi osobami (trenerami), posiadającymi co najmniej 3 letnie doświadczenie w prowadzeniu zajęć o tematyce obsługi komputera , oprogramowania lub technologii informatycznych

9.3 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.

VI. OGÓLNE WARUNKI WYKONANIA I ODBIORU ROBÓT

1. Pozostałe wymagania od Wykonawców

Poza robotami podstawowymi, opisanymi w dokumentacji przetargowej wykonawca jest zobowiązany do skalkulowania wszelkich robót pomocniczych, jakie uzna za niezbędne do prawidłowego wykonania robót dla przyjętej technologii, uwzględniając warunki ich wykonania.

Wykonawca powinien ponadto uwzględnić w cenie – w ramach kosztów dodatkowych – wszelkie pozostałe koszty związane z kompleksową realizacją zamówienia, w tym:

- koszty opracowania planu bezpieczeństwa i ochrony zdrowia oraz wykonania jego zaleceń,
- koszty zużycia mediów niezbędnych na czas budowy,
- koszty zabezpieczenia istniejących elementów obiektu oraz wyposażenia (urządzeń) Użytkownika przed ich zniszczeniem w trakcie wykonywania robót,

- koszty związane z zorganizowaniem pracy w sposób minimalizujący zakłócenie prowadzenia bieżącej działalności Użytkownika,
- koszty urządzenia placu budowy,
- koszty oznakowania robót i zabezpieczenia warunków bhp i ppoż. w trakcie realizacji robót,
- koszty płatnych prób, badań, odbiorów technicznych, zgodnie z wymogami odpowiednich instytucji,
- koszty opracowania dokumentacji powykonawczej,
- koszty uporządkowania oraz przywrócenia obiektu oraz terenu po wykonanych robotach do stanu pierwotnego wraz z naprawą ewentualnych szkód użytkownikowi lub osobom trzecim,
- wszelkie inne koszty wynikłe z analizy dokumentacji projektowej, przyjętej przez Wykonawcę technologii wykonania inwestycji oraz dokonanej wizytacji terenu budowy.

2. Szkolenia dla administratorów sieci

W ramach 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 bezprzewodowa siecią WLAN (kontroler sieci bezprzewodowej)
- Zarządzania systemem LMS
- Polityki autentykacji i autoryzacji użytkowników sieci
- Wykonywania kopii bezpieczeństwa, plików konfiguracyjnych itp.

3. Dokumenty odbioru końcowego

- Dzienniki budowy (jeśli będzie wymagany)
- Oświadczenie kierownika budowy o zgodności wykonania obiektu budowlanego z projektem budowlanym i warunkami pozwolenia na budowę, przepisami i obowiązującymi Polskimi Normami
- Dokumentacja techniczna powykonawcza
- Protokoły odbiorów częściowych
- Protokoły z pomiarów i testów,
- Odpowiednie atesty i certyfikaty
- Instrukcje obsługi, dokumentacje i inne dokumenty dostarczane wraz ze sprzętem, przez producenta
- Listy obecności oraz inna niezbędna dokumentacja związana z przeprowadzonymi szkoleniami dla Beneficjentów projektu

VII. CZĘŚĆ INFORMACYJNA PROGRAMU

1. Akty prawne i rozporządzenia:

- 1.1 „Ustawa Prawo telekomunikacyjne z dnia 16 lipca 2004 roku”.
- 1.2 „Ustawa o wspieraniu rozwoju usług i sieci telekomunikacyjnych (Dz. U.nr 106 z dnia 16 czerwca 2010 r. , poz. 675.)”
- 1.3 „Ustawa o świadczeniu usług drogą elektroniczną z dnia 18 lipca 2002 roku”
- 1.4 „Ustawa o dostępie warunkowym”
- 1.5 „Ustawie z dnia 18 września 2001 r. o podpisie elektronicznym”.
- 1.6 „Ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne z dnia 17 lutego 2005 roku”.

- 1.7 Prawo Ochrony Środowiska z dnia 27 kwietnia 2001r., w zakresie zasad ochrony środowiska oraz warunków korzystania z jego zasobów
- 1.8 Rozporządzenie Rady Ministrów z dnia 21 sierpnia 2007 (Dz. U. 2007 nr 158 poz. 1105)
- 1.9 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.)
- 1.10 Rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 roku w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych,
- 1.11 Rozporządzenie Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych
- 1.12 Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych
- 1.13 Uchwała Sejmu Rzeczypospolitej Polskiej z dnia 14 lipca 2000 r. w sprawie budowania podstaw społeczeństwa informacyjnego w Polsce.

2. Ramy prawne Komisji Europejskiej w sektorze komunikacji elektronicznej

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

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

- 3.1 Recommendation ITU-R 838, Specific Attenuation Model For Rain For Use In Prediction Methods
- 3.2 Rekomendacja (zalecenie) ITU-R P.838-3: „Ścisły (specyficzny) model do zastosowania w metodach przewidywania tłumienia przez deszcz”
- 3.3 Recommendation ITU-R P.676-3, Attenuation By Atmospheric Gases - Rekomendacja (zalecenie) ITU-R P676.3: „Tłumienie przez gazy atmosferyczne”
- 3.4 Recommendation ITU-R Pn 837-1, Characteristics Of Precipitation For Propagation Modelling – Rekomendacja (zalecenie) ITU-R PN 837-1: „Charakterystyki opadów atmosferycznych dla modelowania propagacji”
- 3.5 Recommendation ITU-R P.530-7, Propagation Data And Prediction Methods Required For The Design Of Terrestrial Line-Of-Sight Systems - Rekomendacja (zalecenie) ITU-PN P530-7: „Dane propagacyjne i metody przewidywania wymagane dla projektowania systemów naziemnych z linią bezpośredniej widzialności”