Program Funkcjonalno-Użytkowy

zadania inwestycyjnego pn.

„INTERNET dla wszystkich – umożliwienie dostępu do szerokopasmowego internetu mieszkańcom z terenu gminy Gózd”

ZAMAWIAJĄCY:

Gmina Gózd
ul. Radomska 7
26-634 Gózd

Opis przedmiotu zamówienia wg Wspólnego Słownika Zamówień (CPV):

CPV 32418000-6 - sieć radiowa,
CPV 32420000-3 - urządzenia sieciowe,
CPV 32421000-0 - okablowanie sieciowe,
CPV 32422000-7 - elementy składowe sieci,
CPV 45300000-0 - roboty instalacyjne w budynkach,
CPV 45310000-3 - roboty instalacyjne elektryczne,
CPV 45312330-9 - montaż anten radiowych,
CPV 45314300-4 – instalowanie infrastruktury okablowania,
CPV 71320000-7 – usługi inżynieryjne w zakresie projektowania,
CPV 32500000–8 – urządzenia i artykuły telekomunikacyjne

Spis treści

1 CZĘŚĆ OPISOWA PROGRAMU

Przedmiotem zamówienia jest kompleksowa realizacja zadania pn. „INTERNET dla wszystkich – umożliwienie dostępu do szerokopasmowego internetu mieszkańcom z terenu gminy Gózd""

Zakres projektu składa się następujących zadań:

1. **Budowy elementów pasywnych sieci oraz instalacji teletechnicznych**
   - Budowa masztów antenowych, ew. konstrukcji wsporczych niezbędnych do montażu anten
   - Instalacja szaf zewnętrznych (typu outdoor) lub wewnętrznych, w zależności od potrzeb oraz wykonanie instalacji okablowania sygnałowego pod potrzeby instalacji anten stacji bazowych
   - Instalacja infrastruktury teletechnicznej dla stacji klienckich

2. **Budowy sieci szkieletowej w oparciu o pasmo licencjonowane**
   - Dostawa, instalacja oraz konfiguracja urządzeń radiowych

3. **Budowa Stacji Bazowych punkt-wielopunkt**
   - Dostawa, instalacja i konfiguracja elementów oraz urządzeń stanowiących wyposażenie Stacji Bazowych
   - Dostawa, instalacja i konfiguracja urządzeń sieciowych

4. **Budowa Głównego Węzła Dystrybucyjnego i Centrum Zarządzania siecią szerokopasmową.**
   - Dostawa i instalacja urządzeń aktywnych stanowiących wyposażenie GWD i CZ
   - Dostawa instalacja oraz konfiguracja systemu zarządzania użytkownikami i usługami sieci.

5. **Wdrożenie telefonii VoIP**
   - Dostawa i instalacja centrali VoIP wraz z wyposażeniem.
   - Dostawa i instalacja telefonów IP.
   - Implementacja nowej centrali z obecnie użytkowanym systemem telefonicznym.

Niniejszy program na celu umożliwienie dokonania wyboru najkorzystniejszej oferty na opracowanie dokumentacji projektowej oraz budowy infrastruktury sieci szerokopasmowej Gminy Gózd.

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.

2 OGÓLNE WYMAGANIA ZAMAWIAJĄCEGO

Program funkcjonalno-użytkowy określa wymagania dotyczące zaprojektowania, budowy i przekazania w użytkowanie wszystkich elementów opisywanego systemu. Wykonawca podejmujący się realizacji przedmiotu zamówienia zobowiązany jest do:

- dokonania wizji w terenie, celem szczegółowego zapoznania się z zakresem prac oraz uwarunkowaniami terenowymi,
- opracowania dokumentacji projektowej zgodnie z umową, przepisami techniczno-budowlanymi, wymaganiami określonymi w programie funkcjonalno-użytkowym,
- normami i wytycznymi w tym zakresie,
- opracowania i przedstawienia zamawiającemu do zatwierdzenia szczegółowego harmonogramu prac,
- budowy infrastruktury,
- sporządzenie dokumentacji technicznej powykonawczej,

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

2.1 Ogólne wymagania w zakresie usług i dostępności sieci

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

- Będzie umożliwiał podłączenie stacji końcowych (terminali użytkowników) w promieniu 360 stopni planowanych stacji bazowych
- Zapewnienie dostępności sieci na poziomie 99,9%,
- 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):

2.2 Ogólne wymagania w zakresie technologii sieci bezprzewodowej

Zamawiający wymaga aby został zrealizowany i uruchomiony dostęp do Internetu z wykorzystaniem sieci szerokopasmowej, powinien spełnić następujące wymagania:

- Warstwa szkieletowa sieci powinna być wykonana w oparciu o licencjonowane pasma radiowe,
- Sieć w warstwie dostępowej (Stacje Bazowe) powinny być oparte o topologię Punkt-Wielopunkt w paśmie licencjonowanym
- 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,
- Budowana infrastruktura sieci bezprzewodowej powinna być zarządzana z istniejącego Centrum Zarządzania, zlokalizowanego w budynku Urzędu Gminy Gózd i powinna spełniać następujące wymagania funkcjonalne:
    a. Wszystkie urządzenia radiowe będą zarządzane poprzez scentralizowany system zarządzania w architekturze klient-serwer;
    b. System zarządzania musi obsługiwać protokoły WWW, Telnet oraz SNMP v1 v2c v3;
    c. System zarządzania musi posiadać funkcjonalność serwera Proxy;
    d. System zarządzania musi posiadać możliwość ręcznego oraz automatycznego dodawania urządzeń poprzez broadcast oraz odpowiedzi na ping ICMP;
    e. System zarządzania musi posiadać możliwość importu baz SNMP MIB-1 oraz MIB-2;
    f. System zarządzania musi posiadać możliwość filtrowania adresów IP urządzeń w sieci;
    g. System zarządzania musi posiadać możliwość hierarchicznego podglądu oraz wizualizacji sieci na mapie cyfrowej;
    h. System zarządzania musi posiadać możliwość definiowania trapów dla rejestrowanych zdarzeń i alarmów;
    i. System zarządzania musi posiadać możliwość generowania długoterminowych raportów statystycznych, wydajnościowych oraz trendów;
    j. System zarządzania musi posiadać możliwość zdalnego upgradu oprogramowania urządzeń radiowych;
    k. System zarządzania musi posiadać możliwość konfiguracji profili użytkowników i zarządzania prawami ich dostępu;
    l. System zarządzania musi być dostarczony wraz z niezbędnymi elementami sprzętowymi wymaganymi do jego prawidłowej pracy;

2.3 Ogólne wymagania w zakresie dokumentacji projektowej

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

- ustawy z dnia 7 lipca 1994r. Prawo Budowlane (Dz. U. z 2006r. Nr 156, poz. 1118 ze zm.) oraz wydanych na jej podstawie rozporządzeń,

- ustawy z dnia 16 lipca 2004r. Prawo Telekomunikacyjne (Dz. U. z 2004r. Nr 171, poz. 1800 ze zm.) oraz wydanych na jej podstawie rozporządzeń,
- ustawy z dnia 27 kwietnia 2001r. Prawo Ochrony Środowiska (Dz. U. z 2006r. Nr 129, poz. 902 ze zm.) oraz wydanych na jej podstawie rozporządzeń,
- rozporządzenia Ministra Infrastruktury z dnia 2 września 2004 roku w sprawie szczegółowego zakresu i formy dokumentacji projektowej, specyfikacji technicznych wykonania i odbioru robót budowlanych oraz programu funkcjonalno- użytkowego (Dz. U. z 2004r. Nr 202, poz. 2072 ze zm.),
- powszechnie obowiązującymi przepisami prawa i normami budowlanymi

Roboty budowlane muszą być prowadzone zgodnie z:
- zatwierdzoną przez Zamawiającego dokumentacją projektową,
- przepisami ustawy z dnia 7 lipca 1994r. Prawo Budowlane (Dz. U. z 2006r. Nr 156, poz. 1118 ze zm.),
- przepisami ustawy z dnia 16 lipca 2004r. Prawo Telekomunikacyjne (Dz. U. z 2004r. Nr 171, poz.
- 1800 ze zm.),
- przepisami ustawy z dnia 27 kwietnia 2001r. Prawo Ochrony Środowiska (Dz. U. z 2006r. Nr 129, poz. 902 ze zm.),

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

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

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

3 AKTUALNE UWARUNKOWANIA PRZEDMIOTU ZAMÓWIENIA

W ramach realizowanego projektu, planowana jest budowa infrastruktury teletransmisyjnej i teletechnicznej która zostanie zlokalizowana na wskazanych przez Zamawiającego obiektach/budynkach należących do Gminy Gózd. Ze względu jednak na ukształtowanie i topografię terenu, dopuszcza się wykorzystanie budynków/obiektów nie należących do Gminy. Jednak w pierwszej kolejności należy projektować lokalizację infrastruktury na obiektach należących do Gminy Gózd, a dopiero w następnej kolejności (po wcześniejszym uzgodnieniu z Zamawiającym) na ew. nieruchomościach prywatnych.

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, jeśli z jakiś względów nie będzie możliwości wykorzystania obiektów przeznaczonych na budowę stacji bazowych wskazanych przez Zamawiającego.

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

4 OGÓLNE WŁAŚCIWOŚCI FUNKCJONALNO-UŻYTKOWE

Zadaniem wykonawcy będzie zaprojektowanie, dostawa materiałów i urządzeń, pozyskanie częstotliwości, wykonanie wszelkich prac budowlanych, montażowych i instalacyjnych oraz uruchomienie stacji bazowych w ramach projektu pn. „INTERNET dla wszystkich – umożliwienie dostępu do szerokopasmowego internetu mieszkańcom z terenu gminy Gózd".
Zakres projektu będzie obejmował zatem budowę infrastruktury sieci szerokopasmowej poprzez budowę szkieletu sieci oraz budowę Stacji Bazowych. Końcowym etapem będzie wyposażenie Głównego Węzła Dystrybucyjnego oraz Centrum Zarządzania w sprzęt aktywny sieci oraz serwery usług - instalacja, konfiguracja i integracja systemu zarządzania.

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

Warstwa dystrybucyjna

Warstwa dystrybucji sieci zostanie zbudowany w oparciu o Główny Węzeł Dystrybucji i Centrum Zarządzania siecią zlokalizowany w budynku Urzędu Gminy Gózd oraz co najmniej trzy węzły dystrybucyjne (Stacje Bazowe) zlokalizowane na terenie Gminy Gózd.

W ramach połączeń dystrybucyjnych planuje się wykorzystanie łącz radiowych pracujących w paśmie licencjonowanym o przepustowości co najmniej 100Mb/s.
Zadaniem warstwy dystrybucyjnej sieci jest zapewnienie wysokiej wydajności transmisyjnej i dostępności połączeń dystrybucyjnych dla Stacji Bazowych.

Warstwa dostępowa

Warstwa dostępowa zostanie zbudowana w oparciu o 4 Stacje Bazowe w konfiguracji min. 3x120 stopni. W ramach innego zadania planowane jest podłączenie jednostek klienckich do Stacji Bazowych będących w ich zasięgu bez konieczności rozbudowy infrastruktury.

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

5 SZCZEGÓŁOWE WŁAŚCIWOŚCI I WYMAGANIA FUNKCJONALNO-UŻYTKOWE

5.1 Opracowanie dokumentacji technicznej w zakresie rozbudowy infrastruktury

Wykonawca zobowiązany jest do opracowania projektu sieci radiowej wraz z niezbędną dokumentacją budowlaną (jeśli będzie wymagana) oraz wykonawczą obejmującą budowę infrastruktury.
Dokumentacja ta powinna zwierać:

- projekty budowlane i projekty wykonawcze masztów antenowych, konstrukcji wsporczych – kompletne (wraz z branżami w przypadku konieczności uzyskania pozwolenia na budowę)
- projekt wykonawczy budowy sieci szerokopasmowej składający się z następujących elementów:
  - projekt planowania radiowego dla sieci szkieletowej oraz Stacji Bazowych z zasięgami oraz parametrami radiowymi
  - projekt wykonawczy budowy warstwy dystrybucji i dostępu
  - 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.

Wykonawca zobowiązany jest do zachowania wszelkich, przepisów oraz norm, które są w jakikolwiek sposób związane z wykonywanymi opracowaniami projektowymi i będzie w pełni odpowiedzialny za przestrzeganie ich postanowień podczas wykonywania opracowań projektowych. Wykonawca jest odpowiedzialny za zorganizowanie procesu wykonywania opracowań projektowych, w taki sposób aby założone cele projektu zostały osiągnięte. Wykonawca będzie przestrzegać praw patentowych i będzie w pełni odpowiedzialny za wypełnienie wszelkich wymagań prawnych odnośnie znaków firmowych, nazw lub innych chronionych praw w odniesieniu do projektów, sprzętu, materiałów lub urządzeń użytych lub związanych z wykonywaniem opracowań projektowych. Wszelkie straty, koszty postępowania, obciążenia i wydatki wynikłe lub związane z naruszeniem jakichkolwiek praw patentowych przez Wykonawcę pokryje Wykonawca. Dokumentacja projektowa powinna być wewnętrznie spójna i skorygowana we wszystkich branżach i zadaniach wyżej opisanych. Powinna zawierać optymalne rozwiązania funkcjonalne, techniczne, konstrukcyjne, materiałowe i kosztowe. Wykonawca dokumentacji projektowej powinien uzyskać, własnym staraniem i na własny koszt, wszystkie wymagane przepisami opinie i uzgodnienia.

5.2 Budowa elementów pasywnych sieci oraz instalacji teletechnicznych w obiektach

5.2.1 Budowa masztów antenowych i/lub konstrukcji wsporczych dla stacji bazowych

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

Zaleca się dokonanie wizji lokalnej we wszystkich lokalizacjach, objętych projektem w celu określenia konieczności budowy masztów antenowych o wysokości 12,00 m.

Projekt zakłada, budowę masztów antenowych na istniejących obiektach (budynkach) jednostek podległych:

1/ Urząd Gminy Gózd
2/ ZS Kuczki
3/ PSP Kłonówek
4/ PSP Podgóra

Zgodnie z powyższym wykazem oraz załączonymi projektami budowlanymi wymagana jest budowa 4 szt. masztów antenowych o konstrukcji kratownicowej dla I strefy obciążenia wiatrem. Maszty antenowe, powinny być posadowione na budynkach, ich wysokość powinna wynosić 12,00 m..

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

- System musi umożliwiać dołączenie w późniejszym terminie innych użytkowników sieci.

5.2.2 Instalacja szaf teletechnicznych oraz wykonanie instalacji okablowania zasilającego, sygnałowego oraz logicznego pod potrzeby instalacji wyposażenia węzłów dostępowych

We wszystkich lokalizacjach budowy stacji bazowych (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.

5.3 Budowa sieci dystrybucyjnej

Warstwa dystrybucyjna sieci powinna być oparta o cyfrowe radiolinie klasy operatorskiej o minimalnej przepustowości 100Mb/s, pracujące w paśmie licencjonowanym.

Sieć dystrybucyjne będzie oparta o minimum 4 węzły dystrybucyjne połączone radioliniami cyfrowymi. Węzły te zostaną wyposażone w Stacje Bazowe w topologie Punkt-Wielopunkt.
Lokalizację węzłów dystrybucyjnych (Stacji Bazowych):

1/ Urząd Gminy
2/ PSP Kuczki
3/ PSP Kłonówek
4/ PSP Podgóra

Wyposażenie Stacji Bazowej należy dobrać w taki sposób aby możliwe było podłączenie do sieci wskazanych jednostek podległych Gminy Gózd.
Niniejszy dokument zawiera specyfikację minimalnych wymagań w tym zakresie.

5.3.1 Łącza dystrybucyjne 100 Mb/s - (3 kpl.)

Celem zapewnienia wysokiej jakości oraz bezpieczeństwa połączeń, sieć dystrybucyjna powinna być oparta o łącza klasy operatorskiej o minimalnej przepustowości 100 Mb/s, pracujące w paśmie licencjonowanym.

Wymagania ogólne

- Wykonawca jest zobowiązany do opracowania planowania radiowego i odpowiedni dobór częstotliwości oraz parametrów pracy radiolinii tak aby osiągnąć dostępność pracy 99.995 % średnio rocznie.
- Wykonawca zobowiązany jest do przygotowania stosownej dokumentacji do Urzędu Komunikacji Elektronicznej w celu uzyskania pozwolenia radiowego przez Zamawiającego
- Wykonawca na czas projektu będzie zobowiązany wnieść opłatę do UKE za wykorzystanie pasma licencjonowanego.

Wymagania szczegółowe:

1. Praca w paśmie licencjonowanym;
2. Dostęp czasowy TDD (Time Division Duplex);
3. Zwielokrotnienie OFDM (Orthogonal Frequency Division Multiplexing);
4. Wykorzystanie technik antenowych MIMO 2x2 oraz Diversity;
5. Obsługiwane modulacje BPSK/QPSK/16QAM/64QAM;
6. Adaptacyjna modulacja i kodowanie;
7. Obsługiwane szerokości kanałów 10, 20 MHz;
8. Automatyczne żądanie retransmisji ARQ (Automatic Repeat Request);
9. Symetryczny przydział ruchu;
10. Wbudowane szyfrowanie AES 128;
11. Synchronizacja czasowa;
12. Obsługa QoS poziom 4 zgodnie z 802.1p i Diffserv;
13. Obsługa VLAN 802.1Q, 802.1P, QinQ;
14. Wydajność sprzętowa 400.000 PPS (Packets Per Second);
15. Możliwość lokalnej i zdalnej aktualizacji oprogramowania;
16. Zasilanie PoE 1000BaseT;
17. Pobór mocy <25W;
18. Klasa szczelności IP67;
19. Temperaturowy zakres pracy -35^{0}C do 60^{0}C;
20. Deklaracja zgodności ETSI EN 302 326;
21. Certyfikat CE;

Wymagany jest 36 miesięczny serwis gwarancyjny na wszystkie urządzenia, świadczony w następującym zakresie:

- przyjmowanie zgłoszeń bezpośrednio w godzinach od 8:00-16:00 w dni robocze
- naprawa lub wymiana w następny dzień roboczy od pisemnego zgłoszenia lub mailem)
- prawo do aktualizacji oprogramowania systemowego

5.3.2 Przełączniki szkieletowe 24 porty 10/100/1000 - (3 szt.)

Wymagania ogólne

- Zamawiający oczekuje, że sprzęt dostarczony w ramach realizacji umowy będzie sprzętem nowym, nie używanym (dostarczanym) wcześniej w innych projektach.
- Zamawiający oczekuje, że sprzęt dostarczony w ramach realizacji umowy będzie posiadał świadczenia gwarancyjne oparte na oficjalnej gwarancji świadczonej przez producenta sprzętu.
- Zamawiający oczekuje, że sprzęt dostarczony w ramach realizacji umowy będzie sprzętem zakupionym w oficjalnym kanale sprzedaży producenta. Co zgodnie z opisem wyżej, będzie on sprzętem nowym i posiadającym stosowny pakiet usług gwarancyjnych kierowanych również do użytkowników z obszaru Rzeczpospolitej Polskiej.

Element	Wymagane minimalne parametry techniczne urządzenia
Architektura	• Przełączniki muszą mieć możliwość łączenia w stosy/wieże do 8 przełączników lub budowę modularną, zapewniając możliwość rozbudowy liczby portów w poszczególnych punktach dystrybucyjnych, • Połączenie urządzeń w stos/wieżę powinno zapewniać redundancję - połączenie przełączników w pętlę zwrotną, • Zarządzanie stosem/wieżą poprzez 1 adres IP.
Interfejsy fizyczne	• Minimum 24 porty 10/100/1000 BASE-T RJ45 z technologią auto-sensing, auto-negotiating MDI/MDI-X • Minimum 4 porty uplink 1000Base-X SFP – dopuszcza się wykorzystanie portów podwójnego zastosowania, • Minimum 2 dedykowane porty do łączenia w stos/wieżę nie ograniczające liczby portów dostępowych, • Minimum 1 port konsolowy do zarządzania przełącznikiem.
Montaż	• Standardowy stelaż teletechniczny 19” typu Rack o wysokości nie większej niż 1 U.
Wydajność	• Minimalna przepustowość: 35 Mpps, • Minimalna wydajność przełącznika: 48 Gbps • Minimalna wydajność po łączenia w stosie: 20 Gbps, a w urządzeniach modularnych minimum 20 Gbps pomiędzy modułami.
Zasilanie	• Przełączniki muszą mieć możliwość doposażenia w system redundantnego zasilania.
Rozmiar tablicy adresów MAC	• Minimalna liczba adresów: 8 000.

Sieci VLAN	• Obsługa sieci VLAN zgodnych ze standardem IEEE 802.1Q z pełnym wsparciem dla protokołów GARP i GVRP, • Obsługa minimum 4 000 ID sieci VLAN oraz minimum 255 sieci VLAN aktywnych jednocześnie w pojedynczym stosie.
Funkcje zarządzania	Przełącznik musi obsługiwać następujące funkcjonalności: • SNMP v1/v2c/v3, • Standardowy interfejs wiersza poleceń CLI, • Secure Shell (SSH), • RADIUS, • TACACS+, • Obsługa wielu obrazów oprogramowania z funkcją odtwarzania, • Obsługa wielu plików konfiguracyjnych, • Plik konfiguracyjny w formie tekstowej, • Telnet, • Secure Copy oraz Secure FTP, • Simple Network Time Protocol (SNTP) lub NTP, • RMON – wsparcie dla minimum 4 grup (history, statistics, alarms, events) • Port mirroring w oparciu o protokół SPAN lub równoważny
Protokoły ogólne	Przełącznik musi obsługiwać następujące protokoły i technologie: • LLDP • 802.3ad Link Aggregation, • 802.1D, • 802.1s Multiple Spanning Tree, • 802.1w Rapid re-convergence of Spanning Tree, • 802.3x Flow Control, • IGMPv1,v2,v 3, • IGMP Snooping, • Ramki Jumbo Frames (minimum 9 kB), • Standardowe listy ACL, • Rozszerzone listy ACL, • RIPv1 i RIPv2, • Trasy statyczne, • DHCP/BootP Relay.
Bezpieczeństwo	Przełącznik musi obsługiwać następujące funkcjonalności: • Musi mieć możliwość pracy w architekturze bezpieczeństwa opartej na rolach. Zapewniając ciągłe zarządzanie tożsamością wraz z opartymi na rolach funkcjami uwierzytelniania, autoryzacji, QoS i ograniczania pasma, • Ochrona przed atakami typu DHCP/ARP Spoof Protection,
QoS	Przełącznik musi obsługiwać następujące funkcjonalności: • Obsługa priorytetów zgodna z IEEE 802.1p, • Obsługa minimum 4 kolejek priorytetów na każdym porcie, • Obsługa wielu mechanizmów kolejkowania - minimum SPQ • Obsługa kontroli poziomu pasma wychodzącego i przychodzącego w każdym przepływie, rate-limit dla ruchu wchodzącego i wychodzącego, • Możliwość przypisania ruchu do różnych sieci VLAN
Uwierzytelnianie	• Urządzenie musi obsługiwać następujące metody uwierzytelniania: o poprzez IEEE 802.1x, o wykorzystujące adres MAC, • Obsługa Dynamic VLAN Assignment (RFC 3580),

Gwarancja	• Gwarancja 36 miesięcy producenta obejmująca wysyłkę następnego dnia roboczego, z dostępem do nowych funkcjonalności, wsparcia technicznego przez email, telefon w wymiarze 8x5 oraz aktualizację oprogramowania, na okres nie krótszy niż 5 lat.

5.4 Budowa Stacji Bazowych

Zamawiający zakłada, budowę 4 Stacji Bazowych (ich lokalizacje zostały określone wyżej) w których zostaną zainstalowane urządzenia stanowiące ich wyposażenie.

W warstwie dostępowej sieci wykonawca musi zapewnić urządzenia radiowe, pracujące w paśmie licencjonowanym.

Budowane Stacje Bazowe, powinny być wyposażone w następujący zestaw elementów i urządzeń:
a) w zakresie infrastruktury pasywnej) :

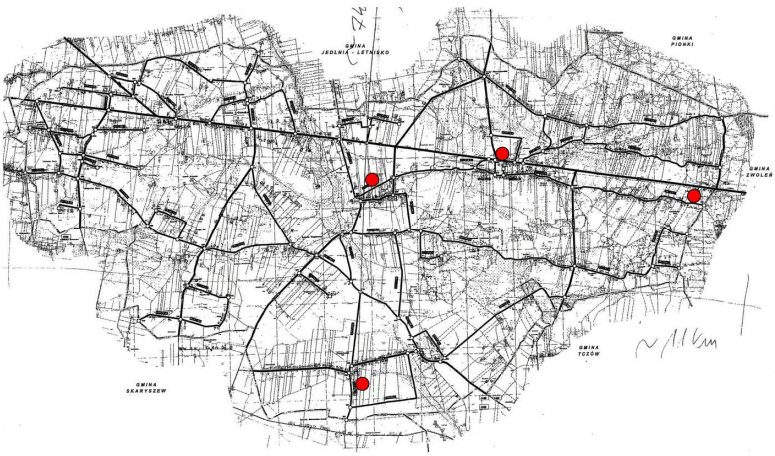
- maszty i/lub konstrukcje wsporcze pod anteny
- szafka dystrybucyjna 19''
- okablowanie zasilające do szaf
- okablowanie sygnałowe/logiczne

b) w zakresie infrastruktury aktywnej

- stacje bazowe systemu Punkt-Wielopunkt
- anteny sektorowe stacji bazowych o azymutach 0, 120, 240 stopni
- urządzenia synchronizacji czasowej
- zarządzalny przełącznik dystrybucyjny (określony wyżej)
- zasilacz awaryjny UPS

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

Poniżej przedstawiono schemat lokalizacji węzłów sieci oraz minimalne wymagania techniczne, funkcjonalne i gwarancyjno- serwisowe poszczególnych elementów i urządzeń do budowy stacji bazowych sieci.



Rys. 1 Schemat lokalizacji węzłów (Stacji Bazowych)

5.4.1 Stacje Bazowe (min. 4 kpl.)

Wymagania techniczne:

1. Wykorzystanie technik OFDM MIMO 2x2 oraz Diversity;
2. Obsługiwane modulacje BPSK/QPSK/16QAM/64QAM;
3. Korekcja błędów FEC k= 1/2, 2/3, 3/4, 5/6;
4. Obsługiwane szerokości kanałów 10, 20 oraz 40MHz;
5. Automatyczny wybór kanałów ACS i żądanie retransmisji ARQ;
6. Adaptacyjna modulacja i kodowanie;
7. Symetryczny przydział ruchu co najmniej 80% w kierunku Downlink;
8. Obsługiwana szerokość ramki 2048 bajtów;
9. Wydajność sprzętowa co najmniej 360.000PPS;
10. Synchronizacja za pomocą GPS;
11. Obsługa Multicast i Broadcast;
12. Możliwość konfiguracji CIR;
13. Obsługa QoS poziom 4 zgodnie z 802.1p i Diffserv;
14. Obsługa VLAN 802.1Q, 802.1P, QinQ;
15. Wbudowany analizator widma;
16. Dostępne interfejsy IDU 1000BaseT oraz SFP;
17. Dostępne złącza antenowe typu N dla anteny sektorowej;
18. Możliwość lokalnej i zdalnej aktualizacji oprogramowania;
19. Zarządzanie za pomocą dedykowanego oprogramowania, przeglądarki internetowej oraz przy pomocy protokołów SNMP v3 oraz Telnet;
20. Zasilanie stacji bazowej poprzez PoE;
21. Pobór mocy urządzeń radiowych <25W;
22. Klasa szczelności urządzeń radiowych IP67;
23. Temperaturowy zakres pracy od -35^{0}C do 60^{0}C;
24. Certyfikat CE;

Wymagania gwarancyjne i serwisowe

Wymagany jest 36 miesięczny serwis gwarancyjny na wszystkie urządzenia, świadczony w następującym zakresie:

- przyjmowanie zgłoszeń bezpośrednio w godzinach od 8:00-16:00 w dni robocze
- naprawa lub wymiana w następny dzień roboczy od pisemnego zgłoszenia lub mailem
- prawo do aktualizacji oprogramowania systemowego

5.4.2 UPS 1000VA RACK - (4 szt.)

Wymagania techniczne

1. Moc pozorna 1000VA
2. Moc rzeczywista 900 Wat
3. Architektura UPS'a line-interactive
4. Minimalny czas podtrzymywania dla obciążenia 100% - 4 min
5. Minimalny czas podtrzymywania dla obciążenia 50% - 12 min
6. Urządzenie musi posiadać układ automatycznej regulacji napięcia AVR
7. Urządzenie musi być wyposażone w port komunikacyjny RS232, port USB, ochronę linii RJ45
8. Urządzenie musi posiadać oprogramowanie do monitorowania parametrów pracy UPSa
9. Urządzenia musi posiadać obudowę typu Rack 19''
10. Maksymalna wysokość urządzenia 2U

Wymagania gwarancyjne i serwisowe

- urządzenia typu UPS muszą być objęte 36-miesięczną gwarancją producenta

5.5 Wyposażenie Głównego Węzła Dystrybucyjnego i Centrum Zarządzania siecią szerokopasmową.

5.5.1 Przełącznik szkieletowy L3 (1 szt.)

Wymagania techniczne

Element	Wymagane minimalne parametry techniczne urządzenia
Architektura	• Przełącznik musi mieć możliwość łączenia w stosy/wieże do 8 przełączników lub budowę modularną, zapewniając możliwość rozbudowy liczby portów w poszczególnych punktach dystrybucyjnych, • Połączenie urządzeń w stos/wieżę powinno zapewniać redundancję - połączenie przełączników w pętlę zwrotną, • Zarządzanie stosem/wieżą poprzez 1 adres IP.
Interfejsy fizyczne	• Minimum 24 porty 10/100/1000 BASE-T RJ45 PoE (zgodnych ze standardem 802.3.af, z technologią auto-sensing, auto-negotiating MDI/MDI-X • Minimum 4 porty uplink 1000Base-X SFP – dopuszcza się wykorzystanie portów podwójnego zastosowania, • Minimum 2 dedykowane porty do łączenia w stos/wieżę nie ograniczające liczby portów dostępowych, • Minimum 1 port konsolowy do zarządzania przełącznikiem.
Montaż	• Standardowy stelaż teletechniczny 19" typu Rack o wysokości nie większej niż 1 U.

Wydajność	• Minimalna przepustowość: 35 Mpps, • Minimalna wydajność przełącznika: 48 Gbps • Minimalna wydajność połączenia w stosie: 32 Gbps
Zasilanie	• Przełączniki muszą być wyposażone w zasilanie PoE niezbędne do zasilania punktów dostępowych WLAN, kamer oraz innych urządzeń PoE w standardzie 802.3af, • Przełączniki dodawane do stosu/wieży muszą zapewniać moc do 540 W dla funkcjonalności PoE, • Przełączniki muszą mieć możliwość doposażenia w system redundantnego zasilania zapewniając zasilanie dla wszystkich portów PoE zgodnie ze standardami 802.3af
Rozmiar tablicy adresów MAC	• Minimalna liczba adresów: 12 000.
Sieci VLAN	• Obsługa sieci VLAN zgodnych ze standardem IEEE 802.1Q, • Obsługa minimum 4 000 ID sieci VLAN oraz minimum 1 000 sieci VLAN aktywnych jednocześnie w pojedynczym stosie.
Funkcje zarządzania	Przełącznik musi obsługiwać następujące funkcjonalności: • SNMP v1/v2c/v3, • Standardowy interfejs wiersza poleceń CLI, • Secure Shell (SSH), • RADIUS, • TACACS+, • Obsługa wielu obrazów oprogramowania z funkcją odtwarzania, • Obsługa wielu plików konfiguracyjnych, • Plik konfiguracyjny w formie tekstowej, • Telnet, • Secure Copy oraz Secure FTP, • Simple Network Time Protocol (SNTP) lub NTP, • RMON – wsparcie dla minimum 4 grup (history, statistics, alarms, events) • Port mirroring w oparciu o protokół SPAN lub równoważny
Protokoły ogólne	Przełącznik musi obsługiwać następujące protokoły i technologie: • LLDP • 802.3ad Link Aggregation, • 802.1D, • 802.1s Multiple Spanning Tree, • 802.1w Rapid re-convergence of Spanning Tree, • 802.3x Flow Control, • IGMPv1,v2,v 3, • IGMP Snooping, • Ramki Jumbo Frames (minimum 9 kB), • Standardowe listy ACL, • Rozszerzone listy ACL, • DHCP/BootP Relay.
Protokoły routingu	Przełącznik musi obsługiwać następujące protokoły routingu: • RIPv1 i RIPv2, • Trasy statyczne, • OSPF, • PIM-SM,

Bezpieczeństwo	Przełącznik musi obsługiwać następujące funkcjonalności: • Musi mieć możliwość pracy w architekturze bezpieczeństwa opartej na rolach. Zapewniając ciągłe zarządzanie tożsamością wraz z opartymi na rolach funkcjami uwierzytelniania, autoryzacji, QoS i ograniczania pasma, • Ochrona przed atakami typu DHCP/ARP Spoof Protection
QoS	Przełącznik musi obsługiwać następujące funkcjonalności: • Obsługa priorytetów zgodna z IEEE 802.1p, • Obsługa minimum 4 kolejek priorytetów na każdym porcie, • Obsługa wielu mechanizmów kolejkowania - minimum SPQ • Obsługa kontroli poziomu pasma wychodzącego i przychodzącego w każdym przepływie, rate-limit dla ruchu wchodzącego i wychodzącego, • Możliwość przypisania ruchu do różnych sieci VLAN
Uwierzytelnianie	• Urządzenie musi obsługiwać następujące metody uwierzytelniania: o poprzez IEEE 802.1x, o wykorzystujące adres MAC, • Obsługa Dynamic VLAN Assignment (RFC 3580),
Gwarancja	• Gwarancja 36 miesięcy producenta obejmująca wysyłkę następnego dnia roboczego, z dostępem do nowych funkcjonalności, wsparcia technicznego przez email, telefon w wymiarze 8x5 oraz aktualizację oprogramowania, na okres nie

5.5.2 Urządzenie bezpieczeństwa sieciowego (1 szt.)

Wymagania techniczne

Element	Wymagane minimalne parametry techniczne urządzenia
Architektura	• System zabezpieczeń musi być dostarczony jako dedykowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze systemu musi występować sprzętowa separacja modułu zarządzania i modułu przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta. • System zabezpieczeń nie może posiadać ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej. • System zabezpieczeń musi działać w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer). Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA. Tryb pracy zabezpieczeń musi być ustalany w konfiguracji interfejsów inspekcyjnych. Musi istnieć możliwość jednoczesnej konfiguracji poszczególnych interfejsów w różnych trybach. • System zabezpieczeń musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive oraz w trybie Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.

Interfejsy fizyczne	• Minimum 8 porów 10/100/1000 BASE-T RJ45, • Minimum 8 portów 1000Base-X SFP, • Minimum 1 port konsolowy do zarządzania urządzeniem
Montaż	• Standardowy stelaż teletechniczny 19” typu Rack o wysokości nie większej niż 1 U.
Funkcjonalność	• System zabezpieczeń musi realizować zadania kontroli dostępu (filtracji ruchu sieciowego), wykonując kontrolę na poziomie warstwy sieciowej, transportowej oraz aplikacji. • System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa). Polityki muszą być definiowane pomiędzy określonymi strefami bezpieczeństwa. • Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ). • System zabezpieczeń musi identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną. • System zabezpieczeń musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia rutingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji. • System zabezpieczeń musi posiadać możliwość uruchomienia modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI (IPS) bez konieczności dokupywania jakichkolwiek komponentów, poza subskrypcją. • System zabezpieczeń musi posiadać możliwość uruchomienia modułu inspekcji antywirusowej, kontrolującego przynajmniej pocztę elektronicznej (SMTP, POP3, IMAP), FTP oraz HTTP i HTTPS bez konieczności dokupywania jakichkolwiek komponentów, poza subskrypcją. Baza AV musi być przechowywania na urządzeniu i regularnie aktualizowana w sposób automatyczny. • System zabezpieczeń musi posiadać możliwość uruchomienia modułu filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupywania jakichkolwiek komponentów, poza subskrypcją. Baza WF musi być przechowywania na urządzeniu i regularnie aktualizowana w sposób automatyczny • System zabezpieczeń transparentnie ustala tożsamość użytkowników sieci (integracja z Active Directory, Citrix, LDAP i serwerami Terminal Services). Polityka kontroli dostępu (firewall) precyzyjnie definiuje prawa dostępu użytkowników do określonych usług sieci i jest utrzymana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie. Ponadto system musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.

Sieci VLAN	• Urządzenie musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez tagowanie zgodne z IEEE 802.1q. • Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3.
Wydajność	• Urządzenie zabezpieczeń musi posiadać przepływność nie mniej niż: o 2 Gb/s dla kontroli firewall (w tym kontrola aplikacji), o 1 Gb/s dla kontroli zawartości (w tym kontrola AV, IPS i WF) o 500 Mb/s dla połączeń IPSec VPN • Urządzenie zabezpieczeń musi obsługiwać nie mniej niż 250 000 jednoczesnych połączeń. • Urządzenie zabezpieczeń musi wspierać minimum 2 000 jednocześnie obsługiwanych tuneli IPSec VPN.
Funkcje zarządzania	• Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI), graficznej konsoli Web GUI oraz scentralizowanego systemu zarządzania. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.
Funkcje routingu	• Urządzenie musi obsługiwać protokoły rutingu dynamicznego, nie mniej niż: o RIP, o BGP, o OSPF. • System zabezpieczeń musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
Funkcje raportowania	• Urządzenie zabezpieczeń musi posiadać wbudowany twardy dysk (minimum 120 GB) do przechowywania logów i raportów. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń.
Bezpieczeństwo	• System zabezpieczeń musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów. • System zabezpieczeń musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege”, tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone. Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama. • System zabezpieczeń musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.

QoS	• System zabezpieczeń musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego.
Gwarancja i serwis	• 36 miesięcy gwarancji • Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim w autoryzowanym ośrodku edukacyjnym. • Wraz z produktem wymagane jest dostarczenie opieki technicznej ważnej przez okres 36 miesięcy. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz jego autoryzowanego polskiego przedstawiciela, wymianę uszkodzonego sprzętu, dostęp do nowych wersji oprogramowania, aktualizację bazy ataków IPS, definicji wirusów oraz bazy kategorii stron WWW, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.

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

Wymagania techniczne:

1. Moc pozorna 3000VA
2. Moc rzeczywista 2600 Wat
3. Architektura UPS'a line-interactive
4. Minimalny czas podtrzymywania dla obciążenia 100% - 5 min
5. Minimalny czas podtrzymywania dla obciążenia 50% - 13 min
6. Urządzenie musi posiadać układ automatycznej regulacji napięcia AVR
7. Urządzenie musi być wyposażone w port komunikacyjny RS232, Port USB, ochronę linii RJ45
8. Urządzenie musi posiadać oprogramowanie do monitorowania parametrów pracy UPSa i być wyposażone w kartę RJ45 umożliwiającą wyłączenie serwerów w przypadku braku zasilania
9. Urządzenie musi posiadać możliwość rozbudowy poprzez dołożenie dodatkowego modułu bateryjnego
10. Urządzenia musi posiadać obudowę typu Rack 19''

Wymagania gwarancyjne i serwisowe

- Urządzenie powinny być objęte minimum 36 miesięczną gwarancją producenta.

5.5.4 Szafa rack

Wymagania techniczne:

1. Szafa serwerowa 42U szer:800 głeb:1000

2. Drzwi tylne i przednie perforowane z blachy, boki z blachy pełnej
3. Cokół 100 mm z możliwością poziomowania

Wyposażenie

1. Panel wentylacyjny dachowy z termostatem i 4 wentylatorami
2. Zaślepka filtracyjna w otworach podstawy szafy
3. Półka 2U 400 mm na urządzenia desktop
4. Półka ruchoma pod klawiaturę
5. Listwa zasilająca 19” z filtrem 2 szt

5.5.5 Serwery i urządzenia dodatkowe

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

Wymagania techniczne (sprzętowe oraz systemowe):

Serwer sieciowy przeznaczony do zapewnienia usług dostępowych dla Beneficjentów sieci	
Płyta główna	- Wieloprocesorowa; - Minimum 7 złącz PCI Express 3 generacji (złącza mogą być uzyskane za pomocą dodatkowych kart) - Zintegrowany układ TPM 1.2.
Procesory	- Zainstalowane procesory osiągające w oferowanym serwerze w testach wydajności SPECint_rate2006 wynik min. 427 pkt;
Pamięć RAM	- Zainstalowane minimum 32 GB pamięci RAM DDR3 LV Registered - Wsparcie dla technologii zabezpieczania pamięci Advanced ECC, Memory Scrubbing; - Minimum 24 gniazda pamięci RAM na płycie głównej, obsługa do minimum 1,5 TB pamięci RAM.
Obudowa	- Typ stelażowy, o maksymalnej wysokości 2U; - Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy
Kontrolery dyskowe	- Zainstalowany kontroler SAS 6G RAID 0,1 z portami wewnątrz obudowy
Dyski twarde	- Zainstalowane 4 dyski SAS 6G o pojemności minimum 900 GB każdy, 10 tys. obr./min., hotplug; - Minimum 8 wnęk dla dysków twardych hotplug 2,5”; - Obsługa dysków SAS, SATA, SSD.
Inne napędy	- Zintegrowany napęd DVD-RW

zintegrowane	
Kontrolery LAN	- zintegrowana dwuportowa 1Gb/s ze wsparciem iSCSI, RJ-45; - dodatkowa 4 portowa karta sieciowa 1Gb/s, RJ45
Porty	- zintegrowana karta graficzna ze złączem VGA (z przodu oraz z tyłu obudowy); - minimum 4x USB 2.0, w tym minimum 2 na panelu przednim, minimum 2 z tyłu obudowy; - 1x RS-232.
Zasilanie, chłodzenie	- Redundantne zasilacze hotplug o sprawności minimum 94% - Redundantne wentylatory hotplug;
Zarządzanie	- Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; • Dedykowana karta 1 Gb/s (dedykowane złącze RJ-45) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania • 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 umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.).
Wspierane systemy	-Windows, VMware, Red Hat Linux, SUSE Linux
Gwarancja	- 3 lata gwarancji producenta serwera, realizowanej w miejscu instalacji sprzętu z gwarantowanym czasem usunięcia awarii następnego dnia roboczego od chwili zgłoszenia. - W przypadku uszkodzenia dysków w okresie gwarancji pozostają one u Zamawiającego.
Inne wymagania	- Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, (ogólnopolski numer o zredukowanej odpłatności 0-800/0-801) w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i

	typ udzielonej gwarancji; - Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;

Wymagania ogólne dotyczące instalacji oprogramowania na serwerach:

Na dostarczonych serwerach należy zainstalować oraz skonfigurować następujące oprogramowanie:

- instalacja oraz konfiguracja środowiska wirtualizacji serwerów w oparciu o dowolne dostarczone rozwiązanie do wirtualizacji.
- utworzenie oraz konfiguracja maszyny wirtualnej dla Systemu zarządzania siecią,
- dostawa, instalacja oraz konfiguracja Systemu zarządzania siecią na maszynie wirtualnej,
- utworzenie oraz konfiguracja maszyny wirtualnej dla Systemu zarządzania kontrolą dostępu do sieci,
- dostawa, instalacja oraz konfiguracja System zarządzania kontrolą dostępu do sieci na maszynie wirtualnej,

5.5.5.2 System zarządzania siecią (1 kpl.)

Element	Wymagane minimalne parametry techniczne
Funkcjonalność	• Musi zapewniać narzędzie do zarządzania na poziomie systemowym - umożliwiające implementacje dowolnej funkcjonalności wynikającej z karty katalogowej zarządzanego urządzenia • Musi umożliwiać centralne wykonywanie operacji systemowych, takich jak wykrywanie urządzeń, zarządzanie zdarzeniami, rejestrowanie zdarzeń i utrzymanie aplikacji • Musi zapewnić narzędzie umożliwiające szybkie i łatwe określenie fizycznej lokalizacji systemów i użytkowników końcowych oraz miejsca ich podłączenia do sieci • Musi zapewniać możliwości monitorowania całego systemu i wdrażania w nim konfiguracji VLAN • Musi zapewniać kompleksowe wsparcie zdalnego zarządzania dla wszystkich proponowanych urządzeń sieciowych, jak również wszystkich urządzeń zarządzanych przez SNMP MIB-I oraz MIB-II • Do obsługi zdalnej nie może wymagać stosowania żadnych klientów użytkowników końcowych lub oprogramowania typu agent • Musi umożliwiać śledzenie atrybutów urządzeń zainstalowanych w sieci, takich jak numer seryjny, etykieta zasobu, wersja oprogramowania *firmware*, typ CPU i pamięć

Architektura	• Musi zapewniać scentralizowane zarządzanie wszystkimi urządzeniami sieci przewodowej. • Musi zawierać zintegrowane aplikacje typu *plug-in*, separujące poszczególne komponenty i uzupełniające możliwości systemu zarządzania. • Musi mieć możliwość instalacji, jako maszyna wirtualna • Musi obsługiwać możliwość automatycznego egzekwowania raz zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej • Rozwiązanie musi integrować się ze środowiskiem wirtualnym: o Musi posiadać wsparcie dla VMware ESX i ESXi o Musi posiadać wsparcie dla Citrix XEN o Musi posiadać wsparcie dla Microsoft HyperV • Obsługa funkcji wysokiej dostępności (High Availability)
Raportowanie	• Musi zapewniać możliwości modyfikacji, filtrowania i tworzenia własnych, elastycznych widoków sieci • Musi umożliwiać prezentowanie danych w formie wykresów lub tabelarycznej i pozwalać użytkownikowi na wybór wielu unikatowych identyfikatorów obiektów (*OID*) • Musi zapewniać dane dla potrzeb audytu (dziennik zdarzeń) • Musi mieć możliwość generowania szczegółowego wykazu produktów zainstalowanych w sieci, zorganizowany według typu urządzenia • Musi rejestrować dane historyczne o atrybutach urządzenia i raportować jakiekolwiek zmiany w urządzeniu • Musi zapewniać dane historyczne o zmianach w konfiguracji i oprogramowaniu *firmware* urządzenia • Musi posiadać centralną bazę, zawierającą historyczne dane związane z operacjami zarządzania, spisem urządzeń • Musi umożliwiać generowanie szczegółowych raportów dla potrzeb związanych z planowaniem spisu urządzeń sieciowych • Musi zapewniać możliwości analiz na poziomie portu • Musi oferować możliwość tworzenia własnych, dostosowanych do potrzeb raportów przez tworzenie indywidualnych szablonów • Możliwość raportowania do elementu zarządzającego maszynami wirtualnymi (vSphere oraz XenCenter), informacji o rzeczywistym położeniu maszyny wirtualnej w sieci- fizyczny port i przełącznik

Narzędzia administracyjne	• Musi pozwalać użytkownikowi na generowanie w tle zaplanowanych zdarzeń i zadań oraz planowanie terminu ich wykonania • Musi zapewnić narzędzie do podglądu i wyboru obiektów MIB *(Management Information Base)* z reprezentacji opartej na drzewie, oraz zawierać kompilator dla nowych lub pochodzących od innych dostawców MIB • Musi pozwalać administratorom IT na desygnowanie wybranego personelu do aktywowania/dezaktywowania wcześniej skonfigurowanych polityk w razie potrzeby • Musi umożliwiać prezentowanie szczegółowych informacji konfiguracyjnych, w tym datę i godzinę zapisów konfiguracji, wersję oprogramowania *firmware* i wielkość pliku konfiguracyjnego • Musi posiadać możliwość pobierania oprogramowania *firmware* do jednego urządzenia lub do wielu urządzeń jednocześnie • Musi mieć możliwość pobierania obrazów *boot PROM* do jednego urządzenia lub do wielu urządzeń jednocześnie • Musi posiadać zdolność do przeprowadzania zaplanowanych, rutynowych kopii zapasowych konfiguracji urządzeń • Musi mieć możliwość pobierania szablonów konfiguracyjnych w formacie tekstowym (ASCII) do jednego lub większej liczby urządzeń • Musi zapewniać interfejs sieci Web zawierający narzędzia do raportowania, monitorowania, rozwiązywania problemów i panele zarządzania • Musi zapewniać oparte o sieć Web elastyczne widoki, widoki urządzeń oraz dzienniki zdarzeń dla całej infrastruktury • Musi umożliwiać diagnozowanie problemów sieciowych i wydajności poprzez analizy danych NetFlow w czasie rzeczywistym
Bezpieczeństwo	• Musi obsługiwać uwierzytelnianie RADIUS i LDAP dla użytkowników aplikacji • Musi obsługiwać bezpieczne zarządzanie przełącznikiem przez https. Musi mieć możliwość definiowania polityk: o ograniczających poziom pasma, o ograniczających liczbę nowych połączeń sieciowych, o ustalających pierwszeństwo ruchu w oparciu o mechanizmy QoS warstw 2 i 3, o nadających tagi pakietom, poddających kwarantannie poszczególne porty lub sieci VLAN i/lub uruchamiających wcześniej zdefiniowane działania • Musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej aplikacji, poprzez wykonanie jednej czynności, dzięki której polityki zostaną rozesłane do wszystkich urządzeń • Musi funkcjonować automatycznie gwarantując, że odpowiednie usługi są dostępne dla każdego użytkownika. Niezależnie od miejsca jego logowania do sieci • Musi współpracować z istniejącymi w danej sieci metodami uwierzytelniania, w szczególności z musi obsługiwać uwierzytelnianie oparte o 802.1X, Radius oraz MAC • Musi mieć możliwość natychmiastowego blokowania lub dopuszczania różnych aktywności sieciowych, w tym dostępu do sieci Web, poczty elektronicznej lub wymiany plików p2p • Musi zapewniać dynamiczne, konfigurowalne rozwiązanie powstrzymywania zagrożeń z szeroką gamą opcji reagowania, rejestrowania i audytowania • Musi natychmiastowo identyfikować fizyczną lokalizację i profil użytkownika źródła ataku • Musi mieć możliwość podejmowania działań w oparciu o wcześniej określone polityki bezpieczeństwa, włączając w to zdolność do powiadamiania systemu IDS o podjętych działaniach poprzez komunikat SNMPv3 *Trap* (*Inform*)

	• Musi umożliwiać automatyczne odłączanie lub izolowanie źródła nielegalnego lub nieodpowiedniego ruchu zidentyfikowanego przez system IDS
Kontrola	• Musi zapewniać szczegółową kontrolę na poziomie portów, opartą na typie zagrożenia i zdarzenia • Musi zapewniać szczegółową kontrolę (każdego użytkownika i aplikacji) nad podejrzanymi działaniami i nieuprawnionym zachowaniem sieci • W przypadku spełnienia wcześniej określonych kryteriów musi mieć możliwość przypisania „roli kwarantanny" użytkownikowi podłączonemu do portu. • Musi umożliwiać izolowanie lub poddawanie kwarantannie atakującego, bez zakłócania pracy innych użytkowników, aplikacji lub systemów krytycznych dla danej organizacji • W przypadku spełnienia wcześniej określonych kryteriów musi dynamicznie odmawiać, ograniczać lub zmieniać parametry dostępu użytkownika do sieci Możliwość przypisywania sieci VLAN, reguł filtrowania warstw L2-L4 oraz QoS na warstwach L2-L4 (DSCP i 802.1p) dla każdej maszyny wirtualnej opartej na przełączniku wirtualnym i wirtualnej grupie portów. Reguły filtrowania na warstwach L3-L4 i reguły QoS muszą obsługiwać zarówno IPv4, jak i IPv6.
Wsparcie dla środowiska wirtualnego	• Możliwość konfiguracji vSwitch i PortGroups w ramach zarządzania maszynami wirtualnymi (vSphere i XenCenter), bez uruchamiania aplikacji do zarządzania maszynami wirtualnymi • Zdolność do ograniczania komunikacji pomiędzy maszynami wirtualnymi Dostarczanie danych historycznych o obecności maszyny wirtualnej (na jakim rzeczywistym porcie oraz przełączniku, i w jakim czasie, dana maszyna wirtualna była obecna). • Dostarczanie informacji o systemie operacyjnym maszyny wirtualnej. Możliwość dostarczenia informacji o stanie zabezpieczeń maszyny wirtualnej, po instalacji specjalnego modułu lub rozszerzeniu licencji. • Możliwość ograniczenia dostępu do określonych zasobów sieci, zgodnie z mechanizmem NAC, tylko dla zatwierdzonych maszyn wirtualnych. W przypadku przyłączenia maszyny wirtualnej do wirtualnej grupy portów lub wirtualnego przełącznika, ruch pochodzący z tej maszyny wirtualnej musi być blokowany, aż do momentu uzyskania odpowiednich praw dostępu dla tej maszyny wirtualnej. • Możliwość ograniczenia dostępu do określonych zasobów sieci zgodnie z mechanizmem NAC, także dla VDI (Virtual Desktop Infrastructure)
Skalowalność	• Aplikacja w momencie dostawy musi obsługiwać minimum 10 urządzeń sieciowych oraz 10 punktów dostępowych • Aplikacja musi umożliwiać przyszłą rozbudowę do minimum 50 urządzeń sieciowych oraz minimum 100 punktów dostępowych
Gwarancja	• 3 letni bezpłatny dostęp do nowych funkcjonalności, wsparcia przez email, telefon i zdalną sesje.

5.5.5.3 System zarządzania kontrolą dostępu do sieci (1 kpl.)

Element	Wymagane minimalne parametry techniczne

Funkcjonalność	Rozwiązanie musi posiadać następujące funkcjonalności: • Aktywne zapobieganie przed dostępem do sieci nieautoryzowanych użytkowników, zagrożonych punktów końcowych i innych niechronionych systemów, • Współpraca z rozwiązaniem Microsoft NAP, • Przypisanie na stałe adresu MAC do określonego przełącznika lub portu przełącznika. Jeżeli system końcowy będzie próbował się uwierzytelnić na innym porcie lub przełączniku, zostanie odrzucony lub przypisana mu zostanie polityka w oparciu o akcje określoną podczas przypisywania mu portu MAC, • Funkcja *IP-to-ID Mapping*, która łączy razem nazwę użytkownika, adres IP, adres MAC oraz port fizyczny każdego punktu końcowego. Ta funkcjonalność jest kluczowa dla potrzeb audytów bezpieczeństwa i analiz dochodzeniowych, • Funkcja portalu rejestracyjnego dla kontroli dostępu, by zapewnić bezpieczne korzystanie z sieci przez gości, bez udziału pracowników działu IT.
Architektura	Rozwiązanie musi posiadać następujące funkcjonalności: • Musi zapewniać rozwiązanie NAC typu *inline* oraz *out-of-band*, które może być zarządzane przez jedną centralną aplikację, • Musi być dostarczone jako maszyna wirtualna • Musi mieć możliwość pracy jako redundantne urządzenia wirtualne w trybie wysokiej dostępności.
Raportowanie	Rozwiązanie musi posiadać następujące funkcjonalności: • Informacje o typie urządzeń działających w sieci oraz określonych potrzebach i zagrożeniach, które są z nimi związane, • Powiadamianie poprzez syslog, pocztę elektroniczną lub usługi webowe o zmianach stanu systemów końcowych, rejestracji gości oraz wynikach skanowania stanu zabezpieczeń systemów końcowych.
Narzędzia administracyjne	Rozwiązanie musi posiadać następujące funkcjonalności: • Musi zapewnić rozwiązanie oferujące jednolity, centralny obraz wszystkich niechronionych elementów związanych z użytkownikami i urządzeniami, który pozwoli później zredukować złożoność procesu zarządzania, • Musi posiadać intuicyjny panel administracyjny, przedstawiający szczegółowy obraz stanu zabezpieczeń podłączonych lub próbujących się podłączyć systemów końcowych, • Musi posiadać funkcję portalu rejestracyjnego dla kontroli dostępu gości, by zapewnić bezpieczne korzystanie z sieci przez gości, bez udziału pracowników działu IT.
Bezpieczeństwo	Rozwiązanie musi posiadać następujące funkcjonalności: • Rozwiązanie musi wykorzystywać oparte na standardach mechanizmy uwierzytelniania dla potrzeb procesów wykrywania, oceniania, kwarantanny, korygowania i autoryzacji podłączanych systemów końcowych, • Rozwiązanie musi obsługiwać uwierzytelnianie RADIUS i/lub LDAP, • Musi umożliwiać ciągłe mechanizmy analizowania zagrożeń, zapobiegania im i przechowywania ich, • Rozwiązanie musi obsługiwać lokalną autoryzację MAC.

Kontrola	Rozwiązanie musi posiadać następujące funkcjonalności: • Zdolność ciągłego przypisywania polityk określonemu użytkownikowi, adresowi MAC lub OUI *(Organizationally Unique Identifier)* adresu MAC, tak aby użytkownik, urządzenie lub grupa urządzeń miały przydzielony ten sam zestaw zasobów sieci, niezależnie od swojej lokalizacji lub konfiguracji serwera RADIUS, • Musi obsługiwać mechanizmy w oparciu o role umożliwiające przepuszczanie lub odrzucanie ruchu sieciowego, nadawanie mu priorytetów, ograniczanie jego szybkości, tagowanie, przekierowywanie i kontrolowanie go w oparciu o tożsamość użytkownika, czas i położenie, typ urządzenia i inne zmienne środowiskowe.
Wsparcie dla środowiska wirtualnego	• Możliwość objęcia mechanizmem NAC maszyn wirtualnych oraz VDI.
Automatyzacja	• Musi zapewniać automatyczne wykrywanie punktów końcowych i śledzenie ich położenia poprzez identyfikowanie nowych adresów MAC i IP, nowych sesji uwierzytelniających (802.1X, wykorzystujące przeglądarkę internetową, Kerberos) lub żądania RADIUS pochodzących z przełączników dostępowych.
Skalowalność	Rozwiązanie musi posiadać następujące funkcjonalności: • Elastyczna obsługa wielu metod uwierzytelniania wielu użytkowników i urządzeń różnych dostawców, • Kontrola dla minimum 500 sesji autentykacyjnych, • System musi umożliwiać przyszłą rozbudowę dla minimum 1 500 sesji autentykacyjnych.
Gwarancja	• 3 letni bezpłatny dostęp do nowych funkcjonalności, wsparcia przez email, telefon i zdalną sesję.

5.6 Wdrożenie telefonii VoIP

5.6.1 Centrala VoIP

5.6.1.1 Jednostka główna

Wymagania techniczne:

- Obsługa łączy zewnętrznych:
  - sieciowanie IP
  - linie operatorów SIP
  - ISDN BRI
  - ISDN PRI
  - standardowe linie analogowe
- Wewnętrzne porty typu: analogowe, cyfrowe, IP oraz ISDN
- Obsługa do minimum 128 wewnętrznych aparatów
- Wbudowana obsługa Call Center
- Wbudowana uproszczona poczta głosowa
- Wbudowana karta DISA z możliwość dostawy modułu DISA jako integralnego elementu jednostki sterującej centrali telefonicznej z możliwością importu plików .wav
- Funkcja odtwarzania przygotowanych plików jako źródła muzyki
- Wbudowany klient SNTP, SNMP,
- Dwa porty LAN RJ45
- Wbudowana funkcja automatycznego trasowania najtańszych połączeń
- Wbudowana funkcja równomiernej dystrybucji połączeń
- Wbudowany system łączności bezprzewodowej DECT:
  - Obsługa do minimum 64 słuchawek
- System obsługi połączeń przychodzących wspomagany funkcją CLIP
- Funkcja automatycznej konfiguracji łącza ISDN
- Wbudowana funkcja CLIP dla wszystkich zewnętrznych i wewnętrznych linii analogowych
- Komunikaty w języku polskim na wyświetlaczach aparatów systemowych
- Systemowa książka telefoniczna na 1000 wpisów
- Optyczna sygnalizacja pozostawionej wiadomości
- Możliwość powiadomienia zajętego abonenta o połączeniu
- Blokowanie połączeń wychodzących
- Możliwość pozostawienia wiadomości
- Obsługa konferencji
- Raporty taryfikacji - z połączeń wychodzących, przychodzących
- Obudowa Rack 19”

Należy dostarczyć licencje umożliwiające korzystanie z Centrali VoIP przez wszystkie urządzenia do niej podłączone

5.6.1.2 Karta analogowa portów wewnętrznych

- Umożliwiająca podłączenie 16 wewnętrznych urządzeń analogowych (telefonów, faksów, modemów)
- Funkcja identyfikacji abonenta dzwoniącego w standardzie FSK na wszystkich portach
- Dioda statusu karty
- 16 gniazd RJ45

5.6.1.3 Karta portów miejskich

- Pozwalająca na podłączenie 8 analogowych linii zewnętrznych
- Wbudowana identyfikacja abonenta dzwoniącego na wszystkich portach w standardzie FSK i DTMF
- Dioda statusu karty

5.6.1.4 Karta VOIP

- Obsługująca minimum 8 kanałów VoIP
- Obsługiwane kodeki: G.711 i G.729A
- Pozwalająca na uruchomienie w systemie:
    - linii zewnętrznych IP (H.323 lub SIP)
    - linii wewnętrznych IP (aparaty SIP i systemowe)
    - anten DECT IP
- Możliwość transmisji faksów T.38

5.6.2 Telefon systemowy IP typ1

Wymagania techniczne:

- Współpracujący z zaoferowaną centralą VOIP
- 3-liniowy, 24-znakowy, podświetlany wyświetlacz alfanumeryczny
- Dwa gniazda RJ45
- Zasilanie PoE lub opcjonalny zasilacz
- Przycisk nawigacyjny
- Funkcja głośno mówiąca
- Gniazdo słuchawki nagłownej
- Regulacja głośności w słuchawce
- Współpraca z opcjami:
    - moduł bluetooth

    - słuchawki nagłowne
- Płynna regulacja kąta pochylenia wyświetlacza

5.6.3 Telefon systemowy IP typ2

Wymagania techniczne:

- Współpracujący z zaoferowaną centralą VOIP
- 16-znakowy alfanumeryczny wyświetlacz
- Dwa gniazda RJ45
- Zasilanie PoE lub opcjonalny zasilacz
- Przycisk nawigacyjny
- Duża lampka dzwonka i oczekującej wiadomości
- Funkcja głośno mówiąca
- Gniazdo słuchawki nagłownej
- 4-poziomowa regulacja głośności w słuchawce
- 8 przycisków programowalnych
- Praca w dwóch położeniach: wysokim i niskim

6 OGÓLNE WARUNKI WYKONANIA I ODBIORU ROBÓT

6.1 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:

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

Uwaga!

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

6.1.1 Szkolenia dla administratorów sieci

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

- Konfiguracji i zarządzania radioliniami cyfrowymi
- Podstawowej konfiguracji i zarządzania urządzeniami aktywnymi sieci

- Administracja i zarządzanie systemem radiowym

6.1.2 Dokumenty odbioru końcowego

Wymagane dokumenty do odbioru końcowego:

- 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

7 CZĘŚĆ INFORMACYJNA PROGRAMU

7.1 Warunki prawne i organizacyjne, jakie należy uwzględnić w projektowaniu i technologicznym wykonaniu zamówienia:

7.1.1 Akty prawne i rozporządzenia:

1.1 „Ustawa Prawo telekomunikacyjne z dnia 16 lipca 2004 roku".

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

1.3 „Ustawa o dostępie warunkowym"

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

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

1.6 Prawo Ochrony Środowiska z dnia 27 kwietnia 2001r., w zakresie zasad ochrony środowiska oraz warunków korzystania z jego zasobów

1.7 Rozporządzenie Rady Ministrów z dnia 21 sierpnia 2007 (Dz. U. 2007 nr 158 poz. 1105)

1.8 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.)

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

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

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

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

7.1.2 Ramy prawne Komisji Europejskiej w sektorze komunikacji elektronicznej

1. 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.);
2. 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.);

3. 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.);
4. 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.) ;
5. 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.);
6. 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.);
7. Rozporządzenie (EC) 2887/2000 o niezależnym dostępie do pętli lokalnych

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

- PN-ETSI EN 302 326-1

  Fixed Radio Systems – Multipoint Equipment and Antennas – Part 1: Overview and Requirements for Digital Multipoint Radio Systems.

- PN-ETSI EN 302 326-2

  Fixed Radio Systems – Multipoint Equipment and Antennas – Part 2: Harmonized EN covering essential requirements under article 3.2 of the R & TTE directive for Digital Equipment of Multipoint Radio Systems.

- PN-ETSI EN 302 326-3

  Fixed Radio Systems – Multipoint Equipment and Antennas – Part 3: Harmonized EN covering essential requirements under article 3.2 of the R & TTE directive for Antennas of Multipoint Radio Systems.

- ITU-R

  Regulations for Radio Communications, Article 5 of the ITU Radio Regulations (Genewa, 2008)

- ECC

  EPORT 91 Compatibility of Earth stations on Board Vessels Transmitting within the GAPS in the CEPT Fixed Service channel plan for the lower 6 GHz band