załącznik nr 1A do SIWZ

INNOWACYJNA GOSPODARKA
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ
ROZWOJU REGIONALNEGO

Zamawiający : **Gmina Wołomin**
ul. Ogrodowa 4
05-200 Wołomin

Temat opracowania:

PROGRAM FUNKCJONALNO – UŻYTKOWY
DLA PROJEKTU :

„Internet szansą rozwoju gminy Wołomin" *realizowanego przez Gminę Wołomin w ramach Działania 8.3. Programu Operacyjnego Innowacyjna Gospodarka na lata 2007-2013"*

Data opracowania :	grudzień 2013
Autor opracowania :	Wacław Olko
Podpis osoby upoważnionej do reprezentowania Zamawiającego :	

Kod zamówienia

1. Usługi inżynieryjne z zakresie projektowania	Kod CPV 71320000-7
2. Wznoszenie masztów antenowych	Kod CPV 45232330-4
3. Wieże , maszty kratowe , półmaszty i słupy stalowe	Kod CPV 44212200-1
4. Sieć radiowa	Kod CPV 32418000-6
5. Sprzęt do przesyłu danych	Kod CPV 32581000-9
6. Serwery sieciowe	Kod CPV 48821000-9
7. Routery sieciowe	Kod CPV 32413100-2
8. Sieć internetowa	Kod CPV 32412110-8
9. Urządzenia sieciowe	Kod CPV 32420000-3
10. Awaryjne urządzenia energetyczne	Kod CPV 31682530-4
11. Instalowanie urządzeń telekomunikacyjnych	Kod CPV 45314000-1
12. Montaż anten radiowych	Kod CPV 45312330-9
13. Telekomunikacyjne roboty dodatkowe	Kod CPV 45232332-8
14. Instalowanie urządzeń klimatyzacyjnych	Kod CPV 45331220-4
15. Roboty instalacyjne elektryczne	Kod CPV 45310000-3
16. Roboty wykończeniowe w zakresie obiektów budowlanych	Kod CPV 45400000-1
17. Instalowanie okablowania komputerowego	Kod CPV 45314320-0
18. Urządzenia komputerowe	Kod CPV 30230000-0
19. Instalacja wyposażenia	Kod CPV 45421153-1
20. Usługi w zakresie napraw i konserwacji i podobne usługi dotyczące komputerów osobistych, sprzętu biurowego, sprzętu telekomunikacyjnego	Kod CPV 50300000-8
21. Usługi w zakresie rozległej sieci komputerowej	Kod CPV 72720000-3
22 Usługi w zakresie wsparcia technicznego	Kod CPV 72611000-6

Zawartość

I. Cześć opisowa programu funkcjonalno-użytkowego

1.1.Opis ogólny przedmiotu zamówienia

Przedmiot zamówienia w ramach realizacji projektu pt. „Internet szansą rozwoju gminy Wołomin" należy wykonać w modelu zaprojektuj i wybuduj .

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

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

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

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

- warstwy szkieletowej
- warstwy dystrybucyjnej
- warstwy dostępowej

1.2 Ogólny zakres zamówienia :

1. Zaprojektowanie i wybudowanie wież/masztów oraz innych niezbędnych konstrukcji wsporczych.
2. Adaptację pomieszczenia na serwerownię wraz instalacją niezbędnych urządzeń sieciowych dla Głównego Węzła Dystrybucyjnego (GWD) i Centrum Zarządzania Siecią (CZS)
3. Wykonanie połączeń i węzłów szkieletowych.
4. Wykonanie połączeń i węzłów dystrybucyjnych, w tym połączeń do 16 jednostek podległych beneficjenta (zwanych dalej JPB)
5. Wykonanie węzłów dostępowych które stanowić będą podstawową infrastrukturę teleinformatyczną zapewniającą dostęp do Internetu dla uczestników projektu .
6. Zakup i instalację zestawów komputerowych oraz radiowych jednostek abonenckich dla uczestników projektu (gospodarstwa domowe)
7. Podłączenie 200 BO oraz 16 JPB do sieci szerokopasmowej

1.3 Szczegółowy zakres robót , dostaw i usług

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

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

3. **Budowy sieci szkieletowej oraz dystrybucyjnej**
   - Dostawa, instalacja oraz konfiguracja radiolinii cyfrowych
   - Dostawa, instalacja oraz konfiguracja połączeń punkt-punkt
   - Wykonanie połączeń dla węzłów szkieletowych i dystrybucyjnych , w tym do 16 jednostek podległych gminy Wołomin

4. **Budowy sieci dostępowej (stacji bazowych LTE oraz w punktów dostępowych WiFi oraz instalacja terminali odbiorczych)**
   - Dostawa, instalacja i konfiguracja elementów oraz urządzeń stanowiących wyposażenie stacji bazowych LTE oraz punktów dostępowych WiFi
   - Dostawa, instalacja i konfiguracja przełączników sieciowych oraz UPS-ów
   - Montaż szaf, wsporników antenowych oraz przygotowanie infrastruktury kablowej w obiektach węzłów dostępowych
   - Dostawa i instalacja i konfiguracja radiowych urządzeń odbiorczych dla 200 BO

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

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

6. **Dostarczenie i instalację zestawów komputerowych oraz oprogramowania do BO.**
- Dostawa i instalacja 200 zestawów komputerowych z oprogramowaniem oraz podłączenie ich do radiowych terminali odbiorczych w wybranych przez Zamawiającego 200 uczestników projektu znajdujących się na terenie objętym projektem w Gminie Wołomin.

7. **Przeprowadzenie wymaganych prób i badań funkcjonowania infrastruktury oraz przygotowanie dokumentów związanych z odbiorem przedmiotu zamówienia i rozpoczęciem eksploatacji sieci internetowej .**

- Przeprowadzenie konfiguracji sieci, sprawdzenia jej funkcjonowania u każdego z użytkowników końcowych.
- Przeprowadzenie testów dla urządzeń transmisyjnych warstwy szkieletowej i dystrybucyjnej
- Przeprowadzenie demonstracji działania systemy monitoringu i zarządzanie siecią i użytkownikami zainstalowanymi w GWD i CZS
- Przygotowanie protokołu odbioru wykonanych w ramach realizacji projektu robót
- Przygotowanie dokumentacji powykonawczej
- Przeprowadzenie szkolenia dla administratorów sieci .

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

- Serwis i utrzymywanie sprzętu komputerowego u BO (200 zestawów komputerowych z dostępem do wybudowanej sieci) wraz z wsparciem technicznym.
- Serwis i utrzymanie wybudowanej infrastruktury sieci szerokopasmowej.

II . OGÓLNE WYMAGANIA ZAMAWIAJĄCEGO

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

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

2.1 <u>W zakresie usług i dostępności sieci</u>

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

- Szybkość łącza do BO min.: 2 Mb/s z możliwością zwiększenia do 8 Mb/s
- Szybkość łącza od BO min.: 512kb/s z możliwością zwiększenia do 2 Mb/s
- Szybkość łącza do JPB min.: 10 Mb/s z możliwością zwiększenia do 50 Mb/s
- Szybkość łącza od JPB min.: 4 Mb/s z możliwością zwiększenia do 20 Mb/s

- Szybkość połączeń szkieletowych : symetrycznie , min. 180 Mb/s
- Szybkość połączeń dystrybucyjnych : symetrycznie ,min. 80 Mb/s
- Zapewnienie dostępności sieci na poziomie min. 99,98% (warstwa dystrybucyjna)
- Zapewnienie dostępności sieci na poziomie min. 99,995% (warstwa szkieletowa)
- Zapewnienie czasu usunięcia uszkodzenia 95% przypadków zgłoszonych usterek w czasie poniżej 48h

- Możliwość ustawienia strony www uruchamianej po zalogowaniu do systemu przez BO
- Możliwość blokowania wybranych stron www
- Możliwość blokady wybranych portów i usług (np. usług wymiany plików)

2.2 W zakresie technologii sieci bezprzewodowej

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

- sieć w warstwie dostępowej powinna być zgodna ze standardem 3GPP LTE pracująca na licencjonowanym pasmie 3,4-3,6 Ghz TDD oraz na technologii 802.11 a/b/g/n (obsługa MIMO) i działać na uwolnionych przez Urząd Komunikacji Elektronicznej częstotliwościach 2,4 Ghz oraz 5,4-5,7 GHz, z zachowaniem obowiązujących przepisów w tym zakresie, w szczególności maksymalnej mocy e,i.r.p.
- wymaga się aby pojedyncze urządzenie punktu dostępowego WIFI posiadało 2 interfejsy radiowe tzw. Dual Band, każdy na inne pasmo uwolnione i bezpłatne w użytkowaniu
- sieć radiowa w warstwie dystrybucyjnej powinna być wykonana i funkcjonować w oparciu o licencjonowane pasmo niezbędne do zapewnienia jakości i pewności połączeń . Jako równoważne dopuszcza się połączenia światłowodowe.
  W uzasadnionych przypadkach dopuszcza się możliwość pracy w oparciu o nielicencjonowane pasmo 5,4 -5,7 GHz
- sieć radiowa w warstwie szkieletowej powinna być wykonana i funkcjonować tylko i wyłącznie w oparciu o licencjonowane pasmo niezbędne do zapewnienia jakości i pewności połączeń . Jako równoważne dopuszcza się połączenia światłowodowe
- węzły dostępowe i dystrybucyjne powinny być wybudowane w pierwszej kolejności na obiektach należących do Gminy Wołomin .
- sieć powinna posiadać wsparcie dla najnowszych technologii bezpieczeństwa w zakresie autentykacji i autoryzacji użytkowników oraz bezpieczeństwa transmisji danych
- sieć powinna posiadać wsparcie dla usług QoS we wszystkich warstwach

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

2.3 . Ogólne wymagania obsługi gwarancyjno-serwisowej

- Wszystkie elementy wchodzące w skład przedmiotu zamówienia powinny być objęte 36 miesięczną gwarancją (o ile szczegółowe zapisy PFU nie stanowią inaczej)
- W okresie gwarancji Wykonawca zobowiązany jest zapewnić Zamawiającemu:

- usuwanie wszelkich wad i nieprawidłowości powstałych na wskutek standardowej i zgodnej z przeznaczeniem eksploatacji przedmiotu zamówienia
- przyjmowanie zgłoszeń serwisowych w godzinach 8.00-18.00 (telefonicznie pod wskazanym przez wykonawcę numerem telefonu) z możliwością zgłaszania awarii bezpośrednio u producenta (na wypadek braku reakcji serwisowej ze strony Wykonawcy)
- dostęp do bezpośredniego wsparcia technicznego producenta

– Jeżeli w trakcie trwania gwarancji, istnieje konieczność wykonywania okresowych przeglądów gwarancyjnych, wówczas przeglądy te będą wykonywane na koszt Wykonawcy.

Szczegółowe warunki w tym zakresie zostały opisane w pkt. 5.7

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

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

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

III. AKTUALNE UWARUNKOWANIA WYKONANIA PRZEDMIOTU ZAMÓWIENIA.

Opis stanu istniejącego.

Gmina Wołomin dysponuje nieruchomościami, na których mogą zostać wybudowane stacje bazowe LTE oraz węzły dostępowe WiFi będące podstawą infrastruktury telekomunikacyjnej zapewniającej dostęp do Internetu. Są to budowle , nieruchomości gruntowe, budynki jednostek podległych oraz inne obiekty będące w dysponowaniu Gminy Wołomin (tabela 1 , tabela 2).
- Wykonawca w pierwszej kolejności będzie projektował konstrukcje na nieruchomościach należących do Gminy Wołomin lub będącym w jej dysponowaniu.
- W następnym kroku, przy ich braku należy wykonać akwizycje innych nieruchomości gruntowych lub obiektów wysokościowych oraz uzyskać akceptację Zamawiającego.

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

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

Gmina Wołomin dysponuje pomieszczeniem na serwerownię (Głównego Węzła Dystrybucyjnego i Centrum Zarządzania Siecią) zlokalizowane w budynku ZEC Wołomin . Wybrane przez Wykonawcę pomieszczenie zostanie udostępnione w celu jego adaptacji oraz wyposażenia przez Wykonawcę.

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

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

Tabela 1 . Zestawienie jednostek podległych które należy podłączyć do sieci

Lp.	Jednostka organizacyjna	Adres
1	Szkoła Podstawowa nr 3 im. J. Piłsudskiego	ul. Piłsudskiego 53, 05-200 Wołomin
2	Szkoła Podstawowa nr 7	ul. Poprzeczna 6, 05-200 Wołomin
3	Zespół Szkół nr 1	ul. Sasina 33, 05-200 Wołomin
4	Zespół Szkół nr 2	Al. Armii Krajowej 81, 05-200 Wołomin
5	Zespół Szkół nr 3	ul. Kazimierza Wielkiego 1, 05-200 Wołomin
6	Zespół Szkół nr 4	ul. 1 Maja 33, 05-200 Wołomin
7	Zespół Szkół nr 5	ul. Lipińska 16, 05-200 Wołomin
8	Zespół Szkół w Duczkach	ul. Szkolna 1, 05-200 Wołomin
9	Zespół Szkół w Osnowie	ul. Matarewicza 148, 05-230 Kobyłka
10	Szkoła Podstawowa w Majdanie	ul. Racławicka 2, 05-200 Wołomin
11	Szkoła Podstawowa w Starym Grabiu	ul. Cichorackiej 25, 05-200 Wołomin
12	Szkoła Podstawowa w Zagościńcu	ul. Szkolna 1, 05-200 Wołomin
13	Ośrodek Pomocy Społecznej w Wołominie	Al. Armii Krajowej 34, 05-200 Wołomin
14	Muzeum im. Wacława i Zofii Nałkowskich	ul. Nałkowskiego 17, 05-200 Wołomin
15	Miejski Dom Kultury w Wołominie	ul. Mariańska 7, 05-200 Wołomin
16	Miejska Biblioteka Publiczna	ul. Wileńska 32, 05-200 Wołomin

Tabela 2 . zestawienie innych jednostek podległych

Lp.	Jednostka organizacyjna	Adres
1	Zespół szkół w Czarnej	Ul. Witosa 52, 05-200 Wołomin
2	Przedszkole nr 2	ul. Polna 32, 05-200 Wołomin

3	Przedszkole nr 5	ul. Broniewskiego 2, 05-200 Wołomin
4	Przedszkole nr 8	ul. Fieldorfa 22, 05-200 Wołomin
5	Przedszkole nr 9	ul. Piłsudskiego 15, 05-200 Wołomin
6	Przedszkole nr 10	ul. Armii Krajowej 56, 05-200 Wołomin
7	Przedszkole w Duczkach	ul. Miła 4, 05-200 Wołomin
8	Urząd Miejski w Wołominie	ul. Ogrodowa 4, 05-200 Wołomin
9	Komin ZEC	ul. Szosa Jadowska 49, 05-20 Wołomin

IV. Ogólne właściwości funkcjonalno-użytkowe.

1)Liczba węzłów dostępowych i wynikająca stąd liczba sektorów radiowych ma być dobrana zależnie od warunków terenowych, obsługiwanej liczby odbiorców co powinno być poparte wynikami planowania radiowego.
2)Sieć dostępowa powinna objąć zasięgiem co najmniej 90% obszaru projektowego ,zamieszkałego co powinno być poparte wynikami planowania radiowego.
3) Sieć radiowa musi być tak zaprojektowana aby każde z połączeń szkieletowych i dystrybucyjnych posiadało odpowiednio zbilansowaną przepływność wynikającą z obciążeń (UL / DL) niezależnie od topologii jej wykonania.

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

5)W projekcie założono, że we wskazanej przez Gminę Wołomin lokalizacji jednostki podległej będzie instalowany punkt dostępowy typu wew. WiFi działający na paśmie 2,4Ghz

6)Adaptacja pomieszczenia na serwerownię polegać będzie na: zainstalowaniu klimatyzacji oraz systemu dostępu, modernizacji sieci elektrycznej w celu jej dostosowania do przewidywanych obciążeń związanych z funkcjonowaniem osprzętu LAN / serwerów, montażu podłogi technicznej , szafy IT wraz zasilaniem awaryjnym.
7) Inne cechy dla całości systemu:
- System powinien umożliwiać dostęp wyłącznie autoryzowanym użytkownikom i stacjom roboczym
- System powinien monitować zamawiającemu próbę podłączenia nieautoryzowanej jednostki lub udostępnienie Internetu poza lokal
- Urządzenia składowe muszą charakteryzować się trwałością funkcjonowania i zapewnić konstrukcyjnie min. 6 letni okres eksploatacji
- Sprzęt oraz zastosowana technologia ma spełniać nowoczesne standardy dla tego typu urządzeń, zarówno co do ich specyfikacji technicznych elementów elektronicznych, teleinformatycznych oraz mechanicznych - minimalne wymagania w tym zakresie zostały określone w dalszej części dokumentu
- System powinien zapewnić skalowalność, w przypadku rozszerzenia projektu o kolejnych beneficjentów.
- Zastosowane urządzenia muszą być fabrycznie nowe i pochodzić z oficjalnego kanału sprzedaży
- System w warstwie dostępowej powinien być typu otwartego przez co rozumie się możliwość zastosowania w przyszłości radiowych terminali klienckich pochodzących od różnych producentów.

V. Szczegółowe właściwości i wymagania funkcjonalno-użytkowe

5.1 Przygotowanie dokumentacji projektowej, harmonogramu prac oraz innej niezbędnej dokumentacji

Dokumentacja projektowa winna być kompletna z punktu widzenia celu, któremu ma służyć oraz spełniać wymogi określone przepisami:
- ustawy z dnia 7 lipca 1994r. Prawo Budowlane (Dz. U. z 2006r. Nr 156, poz. 1118 ze zm.) oraz wydanych na jej podstawie rozporządzeń,
- ustawy z dnia 16 lipca 2004r. Prawo Telekomunikacyjne (Dz. U. z 2004r. Nr 171, poz. 1800 ze zm.) oraz wydanych na jej podstawie rozporządzeń,
- ustawy z dnia 27 kwietnia 2001r. Prawo Ochrony Środowiska (Dz. U. z 2006r. Nr 129, poz. 902 ze zm.) oraz wydanych na jej podstawie rozporządzeń,
- rozporządzenia Ministra Infrastruktury z dnia 2 września 2004 roku w sprawie szczegółowego zakresu i formy dokumentacji projektowej, specyfikacji technicznych wykonania i odbioru robót budowlanych oraz programu funkcjonalno- użytkowego (Dz. U. z 2004r. Nr 202, poz. 2072 ze zm.),
- powszechnie obowiązującymi przepisami prawa i normami budowlanymi

Roboty budowlane muszą być prowadzone zgodnie z:

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

Wykonawca zobowiązany jest do opracowania projektu sieci radiowej wraz z niezbędną dokumentacją budowlaną oraz wykonawczą obejmującą cały teren Gminy Wołomin która powinna zwierać:

- planowanie radiowe (LTE , WiFI , LR)

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

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

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

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

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

5.1.1 Wymagania wobec planowania radiowego

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

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

5.2 Wieże i maszty telekomunikacyjne oraz inne konstrukcje wsporcze

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

Wymagania podstawowe :

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

Wymagania szczegółowe :

Wieża lub maszt dla węzłów dostępowych i dystrybucyjnych …… min.15 kpl

- Wieża lub maszt dostosowany do montażu na gruncie o wysokości do 30 metrów zaprojektowana dla obowiązującej strefy wiatrowej oraz obciążenia użytkowego.
- W uzasadnionych przypadkach dopuszcza się instalacje lekkich masztów na dachach budynków, przy czym wysokość konstrukcji nie może przekroczyć 16 m .
- Wszelkie konstrukcje o wysokości 16 m lub więcej , niezależnie od sposobu posadowienia mogą zostać wykonane jedynie ze stali lub strunobetonu.

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

Wieże lub maszty powinny posiadać drabiny wejściowe , systemy asekuracji oraz pomosty spocznikowe na wysokościach wynikających z przepisów . W przypadku masztów typu lekkiego zaleca się aby prace instalacyjne oraz konserwacyjne prowadzone były przy użyciu podnośnika.

Wsporniki dla radiolinii oraz dla 200 urządzeń abonenckich ……..….. liczba wg. projektu

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

Wymagania gwarancyjne i serwisowe :

Wykonawca udzieli minimum 36 miesięcznej gwarancji na wykonane konstrukcje.

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

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

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

Prace dodatkowe związane z masztami i wieżami

- w przypadku wież / masztów na gruncie należy wykonać badania geologiczne gruntu pod budowę konstrukcji (fundamentów)

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

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

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

5.3 Budowa sieci szkieletowej oraz dystrybucyjnej

5.3.1 Radiolinia min. 200 Mb/s FDX do połączeń szkieletowych …….. **.**min. 2 kpl.

5.3.2 Radiolinia min. 100 Mb/s FDX do połączeń dystrybucyjnych ……min. 5 kpl.

Wymagania ogólne

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

Moduł wewnętrzny

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

Natywny Ethernet

- Natywny Ethernet jest rozumiany jako transport Ethernetu na interfejsie radiowym bez wykorzystania innych technologii jak PDH SDH.
- System powinien oferować transport natywnego Ethernetu w kanałach o szerokości (ETSI) 7-56MHz z przepływnością powyżej 400Mbps.

Modulacja adaptacyjna

- System powinien oferować bezprzerwową modulację adaptacyjną, która zapewni automatyczną zmianę modulacji odpowiednio do warunków propagacyjnych.
- Modulacja Adaptacyjna powinna być dostępna w kanałach o szerokości (ETSI) 7-56MHz.
- Zmiany schematu modulacji w funkcjonalności Modulacji Adaptacyjnej powinny następować

bez przerwy w ruchu zarówno dla części PDH jak i części ruchu Ethernet o wysokim priorytecie.

Moduł zewnętrzny

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

Gwarancja i utrzymanie :

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

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

5.3.3 Bezprzewodowy most radiowy punkt-punkt …….…… min. 10 kpl

Wymagania techniczne

- Urządzenie przeznaczone do zastosowań zewnętrznych typu punkt-punkt (wyposażone w zestaw montażowy),
- Temperatura pracy: od -30C do 75C,
- Wilgotność pracy: 5 to 95%,
- Pamięć: 64MB SDRAM, 8MB Flash,
- Pobór mocy: max. 10 Watt,
- Zasilanie: możliwość zasilania zgodnego z 802.3af,
- Regulacje prawne: CE, RoHS,
- Urządzenie zintegrowane z dwu-polaryzacyjną anteną o zysku minimum 24dBi
    - Częstotliwość pracy: 4.9GHz-6.1GHz
    - Separacja polaryzacji: min. 28dB
    - Max VSRW 1.1:1
    - Szerokość wiązki H: 6 stopni
    - Szerokość wiązki V: 6 stopni
    - Wykonanie z materiału odpornego na promieniowanie UV
- Moduł radiowy o mocy max 27dBm i czułości -96 dBm,
- Urządzenie pracujące w standardzie IEEE 802.11n 2x2 MIMO o zwiększonej wydajności odbiornika i realnej wydajności min. 50 Mbps dla ruchu TCP/IP,
- Pracuje w trybach: router lub bridge,
- Interfejs WiFi wspierający tryby Access Point, Access Point WDS, Client, Client WDS.
- System do centralnego zarządzania min. 10 urządzeniami wraz z niezbędnymi licencjami

Wymagania gwarancyjne

- Urządzenia powinny być objęte minimum 36-miesięczną gwarancją

5.3.4. Przełącznik dystrybucyjny 24 porty 10/100, ……..……..……..min. 16 szt.

Wymagania techniczne:

1. Przełącznik musi być dedykowanym urządzeniem sieciowym o wysokości 1U przystosowanym do montowania w szafie rack.

2. Przełącznik musi posiadać 24 porty dostępowe Ethernet 10/100/1000 Auto-MDI/MDIX.
3. Przełącznik musi być wyposażony w nie mniej niż 4 porty uplink Gigabit Ethernet SFP– (obsługiwane co najmniej TX, SX, LX, LH, a także FX).
4. Przełącznik musi być wyposażony w port konsoli oraz dedykowany interfejs Ethernet do zarządzania OOB (out-of-band).
5. Przełącznik musi być wyposażony w nie mniej niż 1 GB pamięci Flash oraz 512 MB pamięci DRAM.
6. Zarządzanie urządzeniem musi odbywać się za pośrednictwem interfejsu linii komend (CLI) przez port konsoli, telnet, ssh, a także za pośrednictwem interfejsu WWW.
7. Urządzenie musi mieć możliwość łączenia przełączników fizycznych w jeden przełącznik wirtualny, traktowany jako jedno urządzenie logiczne z punktu widzenia protokołów routingu, LACP i Spanning Tree. Maksymalna liczba przełączników obsługiwanych w stosie co njamniej 4szt.
8. Przełącznik musi posiadać architekturę non-blocking. Wydajność przełączania w warstwie 2 nie może być niższa niż 56 Gb/s i 41,7 milionów pakietów na sekundę. Przełącznik nie może obsługiwać mniej niż 16 000 adresów MAC.
9. Przełącznik musi obsługiwać ramki Jumbo (9216 bajtów).
10. Przełącznik musi obsługiwać sieci VLAN zgodne z IEEE 802.1Q w ilości nie mniejszej niż 1024. Przełącznik musi obsługiwać sieci VLAN oparte o porty fizyczne (port-based) i adresy MAC (MAC-based).
11. Urządzenie musi obsługiwać agregowanie połączeń zgodne z IEEE 802.3AD - nie mniej niż 32 grupy LAG, po nie mniej niż 8 portów.
12. Przełącznik musi obsługiwać protokół Spanning Tree i Rapid Spannig Tree, zgodnie z IEEE 802.1D-2004, a także Multiple Spanning Tree zgodnie z IEEE 802.1Q-2003 (nie mniej niż 64 instancje MSTP).
13. Przełącznik musi obsługiwać protokół LLDP i LLDP-MED.
14. Urządzenie musi obsługiwać ruting między sieciami VLAN – ruting statyczny, oraz protokoły routingu dynamicznego: RIP. Ilość tras obsługiwanych sprzętowo nie może być mniejsza niż 6 500.
15. Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3 dla ruchu wchodzącego i wychodzącego. Klasyfikacja ruchu musi odbywać się w zależności od co najmniej: interfejsu, typu ramki Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1P), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP. Urządzenie musi obsługiwać sprzętowo nie mniej niż 8 kolejek per port fizyczny.
16. Urządzenie musi obsługiwać filtrowanie ruchu na co najmniej na poziomie portu i sieci VLAN dla kryteriów z warstw 2-4. Urządzenie musi realizować sprzętowo nie mniej niż 1500 reguł filtrowania ruchu. W regułach filtrowania ruchu musi być dostępny mechanizm zliczania dla zaakceptowanych lub zablokowanych pakietów. Musi być dostępna funkcja edycji reguł filtrowania ruchu na samym urządzeniu.
17. Przełącznik musi obsługiwać takie mechanizmu bezpieczeństwa jak limitowanie adresów MAC, Dynamic ARP Inspection, DHCP snooping.
18. Przełącznik musi obsługiwać IEEE 802.1X zarówno dla pojedynczego, jak i wielu suplikantów na porcie. Przełącznik musi przypisywać ustawienia dla użytkownika na podstawie atrybutów zwracanych przez serwer RADIUS (co najmniej VLAN oraz reguła filtrowania ruchu). Musi istnieć możliwość pominięcia uwierzytelnienia 802.1x dla zdefiniowanych adresów MAC. Przełącznik musi obsługiwać co najmniej następujące typy EAP: MD5, TLS, TTLS, PEAP.
19. Urządzenie musi obsługiwać protokół SNMP (wersje 2c i 3), oraz grupy RMON 1, 2, 3, 9. Musi być dostępna funkcja kopiowania (mirroring) ruchu na poziomie portu i sieci VLAN.
20. Architektura systemu operacyjnego urządzenia musi posiadać budowę modularną (poszczególne moduły muszą działać w odseparowanych obszarach pamięci), m.in. moduł przekazywania pakietów, odpowiedzialny za przełączanie pakietów musi być oddzielony od modułu routingu IP, odpowiedzialnego za ustalanie tras routingu i zarządzanie urządzeniem.
21. Urządzenie musi posiadać mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 20 poprzednich, kompletnych konfiguracji.

Wymagania gwarancyjne

- Urządzenie powinny być objęte minimum 36 miesięczną gwarancją

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

Wymagania techniczne:

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

Wymagania gwarancyjne

- Urządzenie powinny być objęte minimum 36 miesięczną gwarancją.

5.3.6 UPS 1000VA RACK……..min.12 szt.

Wymagania techniczne

- Moc pozorna 1000VA
- Moc rzeczywista 600 W
- Architektura UPSa line-interactive
- Maksymalny czas przełączenia na baterię 1,5 ms
- Minimalny czas podtrzymywania dla obciążenia 100% - 2 min
- Minimalny czas podtrzymywania dla obciążenia 50% - 12 min
- Urządzenie powinno posiadać układ automatycznej regulacji napięcia AVR
- Urządzenie powinno być wyposażone w port komunikacyjny RS232
- Urządzenie powinno posiadać oprogramowanie do monitorowania parametrów pracy UPSa
- Urządzenia powinno posiadać obudowę typu Rack 19''
- Maksymalna wysokość urządzenia 2U

Wymagania gwarancyjne

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

5.4 Budowa węzłów dostępowych sieci

Wymagane jest dostarczenie , instalacja oraz uruchomienie :

- co najmniej 2 stacji bazowych LTE oraz minimum 7 sektorów radiowych (łącznie) ;
- co najmniej 5 punktów dostępowych WiFi oraz minimum 10 sektorów radiowych (łącznie)
- Sieć dostępowa powinna być tak zaprojektowana aby objęła swym zasięgiem 90 % obszaru zamieszkałego w tym 98% wskazanych w załączniku 1 beneficjentów ostatecznych.
- Dodatkowo każda z 16 jednostek podległych (JPB) powinna zostać wyposażona w minimum jeden punkt dostępowy WiFi typu wew.

Wszystkie węzły dostępowe powinny być wyposażone w następujący zestaw elementów i urządzeń:
a) w zakresie infrastruktury pasywnej:
- maszty /wieże telekomunikacyjne /konstrukcje wsporcze dla urządzeń i anten
- szafa dystrybucyjna 19''
- okablowanie logiczne i sygnałowe

b) w zakresie infrastruktury aktywnej
- moduł radiowy LTE TDD 3,5GHz
- moduł Core LTE
- punkt dostępowy WiFi (802.11a/b/g/n MIMO) typu zew.
- punkt dostępowy WiFi (802.11b/g/n MIMO) typu wew.
- anteny sektorowe 3,5GHz LTE wykorzystujące technologię MIMO
- anteny sektorowe zew. 2,4 GHz i 5GHz WiFi wykorzystujące technologię MIMO
- zarządzany przełącznik dostępowy z portami PoE
- zasilacz awaryjny UPS dla punktów dostępowych WiFi
- siłownie z zestawem baterii dla stacji bazowych LTE

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

5.4.1 Przełącznik dostępowy 12 port 10/100/1000 12xPoE ……min. 5 szt.

Wymagania techniczne:

1. Przełącznik musi być dedykowanym urządzeniem sieciowym o wysokości 1U przystosowanym do montowania w szafie rack.
2. Przełącznik musi posiadać 12 porty dostępowe Ethernet 10/100/1000 Auto-MDI/MDIX.
3. Przełącznik musi posiadać nie mniej niż 12 portów dostępowych Power over Ethernet zgodnych z 802.3at, dających moc 30 W na każdym porcie.
4. Przełącznik musi być wyposażony w nie mniej niż 2 porty uplink Gigabit Ethernet SFP– (obsługiwane co najmniej TX, SX, LX, LH, a także FX).
5. Przełącznik musi być wyposażony w port konsoli oraz dedykowany interfejs Ethernet do zarządzania OOB (out-of-band).
6. Przełącznik musi być wyposażony w nie mniej niż 1 GB pamięci Flash oraz 512 MB pamięci DRAM.
7. Zarządzanie urządzeniem musi odbywać się za pośrednictwem interfejsu linii komend (CLI) przez port konsoli, telnet, ssh, a także za pośrednictwem interfejsu WWW.
8. Urządzenie musi mieć możliwość łączenia przełączników fizycznych w jeden przełącznik wirtualny, traktowany jako jedno urządzenie logiczne z punktu widzenia protokołów routingu, LACP i Spanning Tree. Maksymalna liczba przełączników obsługiwanych w stosie co njamniej 4szt.
9. Przełącznik musi posiadać architekturę non-blocking. Wydajność przełączania w warstwie 2 nie może być niższa niż 28 Gb/s i 21 milionów pakietów na sekundę. Przełącznik nie może obsługiwać mniej niż 16 000 adresów MAC.
10. Przełącznik musi obsługiwać ramki Jumbo (9216 bajtów).
11. Przełącznik musi obsługiwać sieci VLAN zgodne z IEEE 802.1Q w ilości nie mniejszej niż 1024. Przełącznik musi obsługiwać sieci VLAN oparte o porty fizyczne (port-based) i adresy MAC (MAC-based).
12. Urządzenie musi obsługiwać agregowanie połączeń zgodne z IEEE 802.3AD - nie mniej niż 32 grupy LAG, po nie mniej niż 8 portów.
13. Przełącznik musi obsługiwać protokół Spanning Tree i Rapid Spannig Tree, zgodnie z IEEE 802.1D-2004, a także Multiple Spanning Tree zgodnie z IEEE 802.1Q-2003 (nie mniej niż 64 instancje MSTP).
14. Przełącznik musi obsługiwać protokół LLDP i LLDP-MED.
15. Urządzenie musi obsługiwać ruting między sieciami VLAN – ruting statyczny, oraz protokoły rutingu dynamicznego: RIP. Ilość tras obsługiwanych sprzętowo nie może być mniejsza niż 6 500.
16. Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3 dla ruchu wchodzącego i wychodzącego. Klasyfikacja ruchu musi odbywać się w zależności od co najmniej: interfejsu, typu ramki Ethernet, sieci VLAN, priorytetu w warstwie 2

(802.1P), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP. Urządzenie musi obsługiwać sprzętowo nie mniej niż 8 kolejek per port fizyczny.

17. Urządzenie musi obsługiwać filtrowanie ruchu na co najmniej na poziomie portu i sieci VLAN dla kryteriów z warstw 2-4. Urządzenie musi realizować sprzętowo nie mniej niż 1500 reguł filtrowania ruchu. W regułach filtrowania ruchu musi być dostępny mechanizm zliczania dla zaakceptowanych lub zablokowanych pakietów. Musi być dostępna funkcja edycji reguł filtrowania ruchu na samym urządzeniu.
18. Przełącznik musi obsługiwać takie mechanizmu bezpieczeństwa jak limitowanie adresów MAC, Dynamic ARP Inspection, DHCP snooping.
19. Przełącznik musi obsługiwać IEEE 802.1X zarówno dla pojedynczego, jak i wielu suplikantów na porcie. Przełącznik musi przypisywać ustawienia dla użytkownika na podstawie atrybutów zwracanych przez serwer RADIUS (co najmniej VLAN oraz reguła filtrowania ruchu). Musi istnieć możliwość pominięcia uwierzytelnienia 802.1x dla zdefiniowanych adresów MAC. Przełącznik musi obsługiwać co najmniej następujące typy EAP: MD5, TLS, TTLS, PEAP.
20. Urządzenie musi obsługiwać protokół SNMP (wersje 2c i 3), oraz grupy RMON 1, 2, 3, 9. Musi być dostępna funkcja kopiowania (mirroring) ruchu na poziomie portu i sieci VLAN.
21. Architektura systemu operacyjnego urządzenia musi posiadać budowę modularną (poszczególne moduły muszą działać w odseparowanych obszarach pamięci), m.in. moduł przekazywania pakietów, odpowiedzialny za przełączanie pakietów musi być oddzielony od modułu rutingu IP, odpowiedzialnego za ustalanie tras routingu i zarządzanie urządzeniem.
22. Urządzenie musi posiadać mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 20 poprzednich, kompletnych konfiguracji.

    Wymagania gwarancyjne

    - Urządzenia powinny być objęte minimum 36-miesięczną gwarancją .

5.4.2 Wymagania minimalne dla stacji bazowych LTE

- System powinien być w podstawowych funkcjonalnościach zgodny ze standardem 3GPP LTE (minimum rel. 8)
- System powinien pracować w zakresie częstotliwości 3,4-3.6GHz.
- System powinien zapewniać co najmniej 9 poziomów obsługi jakości usług (QoS) zgodnie ze standardem 3GPP TS 23.203 Paragraf 6.1.7.2;
- System musi zapewnić stałą obsługę zarówno przy zachowaniu widoczności optycznej pomiędzy stacją bazową a terminalem abonenta – LOS, jak również możliwość pracy bez takiej widoczności - NLOS;
- System powinien posiadać wsparcie dla mobilności (jak określono w standardzie 3GPP LTE), również dla terminali stałych i nomadycznych;
- System powinien wspierać technologię OFDMA dla modulacji w dół sieci (downlink) co może znacznie poprawić przepustowość systemu przy wykorzystaniu ograniczonych zasobów częstotliwości radiowych i powinien wspierać technologię SC-FDMA dla modulacji w górę sieci (uplink) co zmniejsza złożoność projektowania radiowego dla urządzeń mobilnych i zmniejsza ich pobór mocy;
- System powinien być w stanie obsługiwać pasma radiowe o szerokości kanału 5MHz , 10MHz oraz 20MHz bez konieczności wymiany sprzętu.
- System powinien wspierać techniki " Forward Error Correction " (FEC).
- System powinien wspierać elastyczne schematy modulacji MCS z nie mniejszą niż 25 różnymi poziomami. System powinien wspierać modulację QPSK, QAM16 i QAM64 przy użyciu technik korekcji błędów "Cyclic Turbo Code" świadczących modulację QAM64 5/6, zarówno dla kierunku transmisji w dół sieci (downlink) oraz w górę sieci (uplink)
- System powinien wspierać technologię zaawansowanych anten MIMO (2Tx4Rx) po stronie stacji bazowych – przynajmniej dwa oddzielne tory nadawania i cztery oddzielne tory odbioru sygnału
- System powinien obsługiwać technologię "Rx diversity" (MRC) dla kierunku uplink
- System powinien wspierać technikę HARQ.

- Zmiany w systemie modulacji (QPSK, QAM16, QAM64) powinny odbywać się automatycznie i w sposób dynamiczny.
- System stacji bazowej powinien być zasilany napięciem stałym 48VDC
- System powinien wspierać szyfrowanie 128-bitowe AES i algorytmy szyfrowania SNOW 3G;
- Elementy zewnętrzne stacji bazowej powinny być zgodne ze współczynnikiem ochrony co najmniej IP66;
- Wsparcie dla elastycznej konfiguracji współczynnika podziału ramki TDD pomiędzy nadawaniem i odbiorem Dowlink/Uplink., w stosunkach od 40/60 do 90/10 – zgodnie ze specyfikacją i ograniczeniami standardu LTE.

Rdzeń sieci (Core)

- Proponowane rozwiązanie sprzętowe powinno być rozwiązaniem możliwym do umieszczenia w jednej szafie telekomunikacyjnej zawierającym komponenty: MME, HSS, SGW i PDN-GW
- Rozwiązanie EPC (ang. Evolved Packet Core) powinno być możliwie jak najmniejsze, pożądane jest, aby zapewnić upakowanie wszystkich elementów w jednej obudowie o wysokości max. 3U lub też powinno mieć możliwość zintegrowania za stacją bazową (wbudowane EPC w stację bazową).
- Dla zapewnienia redundancji, sprzęt musi być zbudowany zapewniając redundancję we wszystkich niezbędnych przypadkach.
- Oprogramowanie Systemowe powinno być zaprojektowane z wysokim poziomem automatycznej korekcji i mechanizmem zapobiegania błędom
- Oferowane rozwiązanie powinno być w stanie poradzić sobie w sytuacji każdej usterki sprzętu lub elementów oprogramowania, awarii zasilania itp.
- Rozwiązanie powinno osiągnąć 99.999% dostępności.
- Proponowany produkt EPC ma możliwość wsparcia redundancji kart 1+1 oraz ma możliwość wsparcia redundancji interfejsów 1+1 lub posiada możliwość pracy w klastrze zapewniającym możliwość ciągłej pracy.
- Proponowany produkt EPC powinien posiadać skalowalną ilość obsługiwanych użytkowników od 500 do 10 000 przez jedno EPC.
- Jakość Usług:
  1. Wykorzystanie mechanizmu QoS dla proponowanego produktu EPC powinno być zgodne z 3GPP TS 23.401
  2. Proponowany produkt EPC powinien wspierać egzekwowanie polityk QoS.
  3. Proponowany produkt EPC wspiera mechanizm kontroli jakości usług w odniesieniu do klasy usług, oraz typ dostępu na podstawie klasyfikacji ruchu
  4. Proponowany produkt EPC lub eNodeB wspiera kolejkowanie ruchu i kształtowanie.
  5. Proponowana produkt EPC lub eNodeB wspiera funkcjonalność kontroli pasma, które mogą być konfigurowane przez operatora sieci.
  6. Proponowany produkt EPC lub eNodeB posiada funkcjonalność kształtowania ruchu.
- Bezpieczeństwo :
  1. EPC dostarcza ochronę szyfrowania SSLv3.0/TLSv1.0/TLSv1.1 pomiędzy siecią NMS i Rdzeniem.
  2. Wszelka sygnalizacja i dane są szyfrowane w celu ochrony integralności dla systemu zarządzania.
  3. Powinna być wspierana funkcjonalność gdzie nieuprawniona strona nie ma możliwości uzyskać dostępu do informacji o systemie i autoryzacji użytkownika.
  4. Proponowana sieć EPC powinna dostarczać logi dziennika dla wszystkich zdarzeń związanych z bezpieczeństwem i powinna zebrać logi w systemie sterowania. Tymczasem wszelkie wykrywanie włamań są zgłaszane do systemu sterowania.
- Transportowanie:
  1. EPC powinna wspierać trunki portu lub pracować w topologii klastra automatycznie przejmując zadania uszkodzonych elementów, aby uniknąć awarii sieci.
  2. EPC GW powinno być wyposażone w interfejs optyczny 10GE lub mieć możliwość pracy w klastrze w ten sposób, by obsłużyć zagregowany ruch i zapewnić redundancję połączeń

Inne wymagania minimalne dla stacji bazowych LTE

- Jednostka podstawowa stacja bazowej powinna obsługiwać kanał o szerokości 20MHz w jednej głowicy radiowej
- Moc transmisyjna nadajnika radiowego mierzona na porcie RF anteny nie może być mniejsza niż 36 dBm na kanał radiowy.
- System stacji bazowej powinien być wyposażony, w co najmniej 1 interfejs RJ45 GE (gigabit ETH);
- System stacji bazowej powinien być wyposażony, w co najmniej 1 interfejs optyczny GE
- Synchronizacja pomiędzy stacjami bazowymi powinna być dokonywana za pomocą GPS lub IEEE 1588-2008
- Stacja bazowa powinna wspierać kontrolę mocy terminali (Uplink Power Control);
- Stacja bazowa powinna wspierać statyczne zabezpieczenie przeciw zakłóceniami miedzy-komórkowymi w kierunku uplink / downlink;
- Temperatura otoczenia, w której stacja bazowa powinna działać prawidłowo, powinna wynosić co najmniej: -30℃ do 55℃

Po ukończeniu budowy węzłów dostępowych (stacji bazowych) Wykonawca zobowiązany jest do wykonania dokumentacji powykonawczej zgodnej z projektem sieci i wykonania dokumentacji zdjęciowej każdej zainstalowanej stacji bazowej.
Po zestawieniu i uruchomieniu stacji bazowych należy przeprowadzić pomiar poziomu sygnału zainstalowanych stacji bazowych, każdego z sektorów osobno. Pomiary zestawione zostaną w formie tabelarycznej oraz na mapach. W tabelach zestawione zostaną współrzędne geograficzne oraz poziom sygnału (minimum 10 pomiarów dla każdego sektora).
Wykonawca jest zobowiązany złożyć wraz z ofertą specyfikację oferowanego systemu w postaci karty katalogowej

Wymagania gwarancyjne

- Urządzenia powinny być objęte minimum 36-miesięczną gwarancją .

5.4.3 Bezprzewodowy punkt dostępu 802.11a/b/g/n ……min.5 szt.

Wymagania techniczne

- Obsługa WDS
- Obsługiwane standardy radiowe:
  - 802.11 a/b/g/n, jednoczesna obsługa minimum 16 ssid
  - moc interfejsów radiowych 20dBm, per antena z możliwością zmniejszenia poziomu
  - obsługa DFS
  - obsługa co najmniej 2x2 MIMO
- Ilość portów:
  - Minimum jeden port RJ-45 auto-sensing 10/100/1000 port (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE802.3ab Type 1000Base-T), umożliwiający pracę w trybie half/full duplex
  - Konsolowy port do zarządzania RJ45
- Urządzenie z możliwością podłączenia anten MIMO w paśmie 2,4Ghz oraz 5Ghz
- Możliwość uruchomienia równoważonego obciążenia AP opartego o zdefiniowane limity ilości podłączonych urządzeń końcowych lub limitu transferu danych
- Obsługiwana prędkość radiowa do 450Mbps na każdy moduł radiowy
- Pamięć RAM minimum 256MB
- Pamięć flash minimum 32MB
- Możliwość podłączenia zewnętrznego zasilacza AC 230VAC
- Obsługa zasilania zgodnego z 802.3af
- Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.

Wymagania gwarancyjne

- urządzenia powinny być objęte minimum 36-miesięczną gwarancją.

5.4.4 Anteny do punktów dostępowych ……..…….min.10 szt.

Wymagania techniczne

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

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

Wymagania gwarancyjne

- anteny powinny być objęte minimum 36-miesięczną gwarancją

5.4.5 Bezprzewodowy punkt dostępu 802.11 b/g/n ……..min.16 szt.

- Interfejs Ethernet: 10/100/1000 Base-T Ethernet
- Zasilanie realizowane przez kabel Ethernet lub zewnętrzne źródło zasilania 48V
- Protokołów sieci bezprzewodowej: IEEE 802.11b/g/n oraz IEEE 802.11i WPA2
- Możliwość agregacji pakietów AMSDU, AMPDU
- Możliwość uruchomienia niezależnych trzech sieci SSID
- Izolacja ruchu pomiędzy poszczególnymi klientami radiowymi
- Zintegrowana fabrycznie w obudowie urządzenia antena pracująca w polaryzacji pionowej i poziomej, w konfiguracji 2x2 MIMO, z przeznaczeniem do zawieszenia urządzenia na suficie.
- Zakres częstotliwości pracy: 2412 – 2472 MHz z regulowana mocą nadawania, jednak nie większą niż + 20 dBm EIRP
- Regulowana szerokość kanału radiowego w zakresie co najmniej: 20MHz, 40MHz
- Obsługiwane techniki modulacji – co najmniej: DSSS (CCK, DQPSK, DBPSK), OFDM (BPSK, QPSK, 16-QAM, 64-QAM)
- Kształtowanie przepustowości (Uplink i Downlink – niezależnie)
- Wbudowany firewall
- Port konsolowy RJ45 lub RS232 z obsługą przez telnet
- Wbudowany serwer WWW z obsługą przez HTTP i HTTPS
- Wbudowany agent SNMP
- Zgodność z obowiązującymi normami w UE dla transmisji w paśmie nielicencjonowanym, posiadanie znaku CE

  Wymagania gwarancyjne

  - Urządzenia powinny być objęte minimum 36-miesięczną gwarancją .

5.4.6 UPS 1000VA RACK……..……..min.5 szt.

Wymagania techniczne

- Moc pozorna 1000VA
- Moc rzeczywista 600 W
- Architektura UPSa line-interactive
- Maksymalny czas przełączenia na baterię 1,5 ms
- Minimalny czas podtrzymywania dla obciążenia 100% - 2 min
- Minimalny czas podtrzymywania dla obciążenia 50% - 12 min
- Urządzenie powinno posiadać układ automatycznej regulacji napięcia AVR
- Urządzenie powinno być wyposażone w port komunikacyjny RS232
- Urządzenie powinno posiadać oprogramowanie do monitorowania parametrów pracy UPSa
- Urządzenia powinno posiadać obudowę typu Rack 19''
- Maksymalna wysokość urządzenia 2U

Wymagania gwarancyjne

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

5.4.7 Siłownia wraz z systemem zasilania do stacji bazowych LTE …….min. 2 kpl

Wymagania techniczne

- system składa się z modułu monitoringu stanu oraz 3 modułów zasilających po 1500W każdy (48V),
- wymagana instalacja co najmniej 2 modułów,
- każdy z modułów jest wykonany w technologii tranzystorowej hot plug & play.
- moduły pracują w systemie redundantnym (n+1).

Parametry wejściowe zasilaczy:

- zakres napięć: 90 - 280 Vrms,
- prąd max: 10A,
- zakres częstotliwości: 45 / 65 Hz,

Parametry wyjściowe zasilaczy:

- napięcie nominalne: 53,5 Vdc,
- zakres napięć: 42 - 58 Vdc,
- prąd max: 30A,
- sygnalizacja stanu: LED,
- temperatura pracy: Od -40ºC do +70ºC,

Parametry akumulatorów siłowni:

- pojemność nominalna: nie mniej niż 50Ah,
- łączna wysokość użytkowa: nie więcej niż 7U,
- żywotność nominalna: co najmniej 10 lat,
- zakres temperatury pracy od -20℃ do +55℃,

Wymagania gwarancyjne

- Urządzenia powinny być objęte minimum 36-miesięczną gwarancją .

5.4.7. Urządzenia abonenckie LTE …… min.162 szt

- Terminale abonenckie być w pełni zgodne ze standardem 3GPP LTE (Rel 8).
- Terminale abonenckie powinny pracować w paśmie częstotliwości 3,4-3.6GHz oraz zapewnić właściwe funkcjonowanie systemu stacji bazowej
- Terminale abonenckie muszą wspierać technologię OFDMA i SC-FDMA

- Terminale abonenckie powinny działać w technologii TDD.
- Terminal abonencki powinien obsługiwać modulacje QPSK, QAM16 i QAM64.
- Terminale abonenckie muszą posiadać wewnętrzną, wbudowaną antenę (z zyskiem nie mniejszym niż 11dBi) lub możliwość instalacji zewnętrznej anteny.
- Maksymalna moc transmisji mierzona w terminalu abonenckim na złączu portu antenowego RF nie powinna być mniejsza niż 21 dBm.
- Terminale abonenckie powinny obsługiwać technologię MIMO.
- Terminale abonenckie powinny być zarządzane lokalnie lub zdalnie za pomocą standardowej przeglądarki internetowej.
- Terminale abonenckie powinny wspierać protokół TR-069 dla administracji centralnej.
- Terminale abonenckie powinny wspierać szyfrowanie 128bit AES i algorytmy szyfrowania SNOW 3G dla LTE.
- Temperatura otoczenia, w której terminal abonencki powinien działać prawidłowo, powinna wynosić, co najmniej: od 0C do +40C dla wewnętrznej części terminala (IDU) i od -30C do +55C dla zewnętrznej części zewnętrznej (ODU).
- Terminale abonenckie powinny być wyposażone w interfejs Ethernet (RJ-45) z PoE (zwany Power over Ethernet).
- Elementy zewnętrzne terminala powinny być zgodne ze współczynnikiem ochrony co najmniej IP55
- Urządzenie powinno mieć wbudowane zabezpieczenie anty-przepięciowe.

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

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

Wymagania techniczne

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

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

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

Wymagania techniczne

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

- Zakres obsługiwanych częstotliwości: Zakres obsługiwanych częstotliwości: Europa (ETSI): 2400-2483,5 MHz (13 kanałów)
- Typ modulacji : BPSK, QPSK, 16QAM, 64QAM, HT20, HT40

- Szerokość kanału możliwość ustawienia : 5/10/20/40 MHz
- Zintegrowana antena panelowa dual polar 14 dBi
- Temperatura pracy: -30℃ - +55℃

Wymagania gwarancyjne i serwisowe

- terminale powinny być objęte minimum 36-miesięczną gwarancją

5.5 Wyposażenie Głównego Węzła Dystrybucyjnego i Centrum zarządzania siecią szerokopasmową.

5.5.1 Adaptacja pomieszczenia przeznaczonego na Centrum Zarządzania Siecią szerokopasmową

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

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

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

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

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

Wymagania ogólne dla system dostępu

- System kontroli dostępu powinien być zrealizowany na bazie urządzeń, które będą pozwalać na rejestrację i podgląd zdarzeń wejścia i wyjścia na kontrolowanym przejściu.
- Zdarzenia te powinny być przesyłane do komputera po sieci lokalnej Ethernet.
- System powinien umożliwiać dostęp poprzez wykorzystanie kart zbliżeniowych oraz manipulatora numerycznego.
- System powinien być wyposażony w dodatkowe elementy pozwalające na ochronę pomieszczenia przed niepowołanym dostępem oraz innymi zjawiskami losowymi.
- Na te elementy składają się:
  - Czujnik otwarcia drzwi
  - Czujnik zbicia szkła
  - Sygnalizacja akustyczno optyczna

- System kontroli powinien w sytuacji wykrycia niepowołanego dostępu dokonać alarmowania poprzez uruchomienie sygnalizatora akustyczno optycznego, jak również wysłanie powiadomienia do odpowiednich osób poprzez sieć GSM.
- Należy również dokonać integracji tego systemu z systemem CCTV, w taki sposób, aby detekcja ruchu lub inny zdarzenie wywołujące alarm powodowało włączenie rejestracji zapisu obrazu z kamery usytuowanej w pomieszczeniu lub przed wejściem do niego

Wymagania techniczne:

System kontroli dostępu należy oprzeć na cyfrowej centrali umożliwiającej współpracę zarówno z czujnikami detekcji sygnałów zewnętrznych jak również z urządzeniami kontroli przejść. Centralę należy zainstalować w obudowie natynkowej wyposażonej w transformator oraz akumulator min. 7 Ah. Kontrola przejścia powinna zostać zrealizowana za pomocą zwory elektromagnetycznej zamontowanej w ościeżnicy drzwi. Jeżeli będą zastosowane metalowe drzwi antywłamaniowe, to należy rozważyć montaż rygla elektromagnetycznego zamiast zwory. Zarówno zwora jak i rygiel powinny pracować w trybie rewersowym, oznacza to , że w normalnym trybie pracy urządzenia te powinny być zasilane napięciem, co spowoduje blokadę drzwi. W trybie otwarcia drzwi urządzenia ryglujące powinny być w stanie jałowym. Przy drzwiach wejściowych należy umieścić czytnik linii papilarnych lub kart zbliżeniowych oraz manipulator. Manipulator należy montować w kasecie natynkowej zamykanej na kluczyk. Manipulator oraz kaseta powinny zostać wyposażone w styk antysabotażowy. Po przyłożeniu karty zbliżeniowej lub zeskanowaniu linii papilarnych do czytnika powinno nastąpić zwolnienie zwory i uzyskanie dostępu do pomieszczenia. Takie zdarzenie dostępu powinno zostać zarejestrowane w buforze centrali i przesłane do systemu monitorującego przejścia. System powinien umożliwiać przegląd zdarzeń i weryfikacje użytkowników wchodzących do pomieszczenia, z możliwością odczytania tych zdarzeń na co najmniej 1 miesiąc wstecz. Wyjście z pomieszczenia powinno następować po wciśnięciu przycisku wewnątrz pomieszczenia. Nie jest wymagana rejestracja wyjścia z pomieszczenia. System powinien być wyposażony w dodatkowe czujniki monitorujące stan otoczenia. Centrala w stanie zazbrojenia powinna reagować na zdarzenia niepowołanego dostępu poprzez zastosowanie czujników ruchu, otwarcia drzwi, zbicia szyby. Każde zarejestrowane zdarzenie naruszenia strefy chronionej powinno generować alarm akustyczno optyczny, jak również wysyłać komunikat do centrum powiadamiania lub do przydzielonych numerów telefonicznych z wykorzystaniem linii analogowej. System powinien umożliwiać przyłączenie do niego zewnętrznej linii telefonicznej analogowej. System powinien zostać wyposażony również w czujnik dymu, co powinno dawać dodatkową możliwość alarmowanie o zagrożeniu pożarowym do centrali alarmowej lub do centrali p.poż. Proponowany system kontroli dostępu powinien charakteryzować się modularnością, możliwością jego rozbudowy i modyfikacji. Powinien dawać możliwość rozbudowy systemu o dodatkowe przejścia jak również dodatkowe elementy ochrony, nie powinien to być system zamknięty. Powinien dawać możliwości konfiguracyjne pozwalające na dostosowanie parametrów pracy do indywidualnych wymagań.

Wymagania formalne gwarancyjne i serwisowe

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

5.5.2 Przełącznik szkieletowy L3 …….. 1 szt.

Wymagania techniczne

1. Przełącznik musi być dedykowanym urządzeniem sieciowym o wysokości max.1U przystosowanym do montowania w szafie rack.
2. Przełącznik musi posiadać 24 porty dostępowych Ethernet 10/100/1000 Auto-MDI/MDIX.
3. Przełącznik musi posiadać nie mniej niż 24 portów dostępowych Power over Ethernet zgodnych z 802.3at, dających moc 30 W na każdym porcie.
4. Przełącznik musi być wyposażony w nie mniej niż 2 porty uplink 10 Gigabit Ethernet SFP+. Wszystkie porty dostępowe 10/100/1000 muszą być aktywne po wyposażeniu przełącznika w moduł uplink. Moduł uplink musi być wymienny „na gorąco (hot-swappable). Moduł uplink SFP

musi akceptować również minimum cztery wkładki SFP umożliwiając obsługę połączeń uplink Gigabit Ethernet.

5. Przełącznik musi umożliwiać stworzenie stosu non-blocking (w postaci pętli) liczącego nie mniej niż 10 urządzeń. Do łączenia w stos muszą być zastosowane dedykowane porty przełącznika o przepustowości nie mniej niż 32 Gb/s. Do każdego przełącznika musi być dołączony kabel do łączenia w stos. Przełącznik musi również udostępniać możliwość podłączenia do stosu portami uplink 10 Gb/s. Stos musi być widoczny z punktu widzenia zarządzania oraz innych urządzeń sieciowych jako jedno urządzenie. Zarządzanie wszystkimi przełącznikami w stosie musi się odbywać z dowolnego przełącznika będącego częścią stosu. Stos musi być odporny na awarie, tzn. przełącznik kontrolujący pracę stosu (master) musi być automatycznie zastąpiony przełącznikiem pełniącym rolę backup'u – wybór przełącznika backup nie może odbywać się w momencie awarii przełącznika master.
6. Przełącznik musi posiadać wymienny zasilacz AC oraz być wyposażony w redundantny zasilacz. Urządzenie musi posiadać wymienny moduł wentylacji. Urządzenie musi posiadać panel LCD z przyciskami, pozwalający na wykonywanie podstawowych czynności związanych z zarządzaniem (adresacja IP, reset).
7. Przełącznik musi być wyposażony w port konsoli oraz dedykowany interfejs Ethernet do zarządzania OOB (out-of-band).
8. Przełącznik musi być wyposażony w nie mniej niż 1 GB pamięci Flash oraz 1 GB pamięci DRAM.
9. Zarządzanie urządzeniem musi odbywać się za pośrednictwem interfejsu linii komend (CLI) przez port konsoli, telnet, ssh, a także za pośrednictwem interfejsu WWW.
10. Przełącznik musi posiadać architekturę non-blocking. Wydajność przełączania w warstwie 2 nie może być niższa niż 88 Gb/s i 65 milionów pakietów na sekundę. Przełącznik nie może obsługiwać mniej niż 32 000 adresów MAC.
11. Przełącznik musi obsługiwać ramki Jumbo (9216 bajtów).
12. Przełącznik musi obsługiwać sieci VLAN zgodne z IEEE 802.1q w ilości nie mniejszej niż 4096. Przełącznik musi obsługiwać sieci VLAN oparte o porty fizyczne (port-based) i adresy MAC (MAC-based). W celu automatycznej konfiguracji sieci VLAN, przełącznik musi obsługiwać protokół GVRP.
13. Urządzenie musi obsługiwać agregowanie połączeń zgodne z IEEE 802.3ad - nie mniej niż 64 grupy LAG, po nie mniej niż 8 portów.
14. Przełącznik musi obsługiwać protokół Spanning Tree i Rapid Spannig Tree, zgodnie z IEEE 802.1D-2004, a także Multiple Spanning Tree zgodnie z IEEE 802.1Q-2003 (nie mniej niż 64 instancje MSTP).
15. Przełącznik musi obsługiwać protokół LLDP i LLDP-MED.
16. Urządzenie musi obsługiwać ruting między sieciami VLAN – routing statyczny, oraz protokoły rutingu dynamicznego: RIP, OSPF, oraz musi posiadać możliwość obsługi protokołów IS-IS i BGP. Ilość tras obsługiwanych sprzętowo nie może być mniejsza niż 10 000. Urządzenie musi obsługiwać protokoły rutingu multicast, nie mniej niż IGMP i PIM-SM.
17. Przełącznik musi obsługiwać mechanizm wykrywania awarii BFD, oraz pozwalać na stworzenie klastra HA z wykorzystaniem protokołu VRRP.
18. Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3 dla ruchu wchodzącego i wychodzącego. Klasyfikacja ruchu musi odbywać się w zależności od co najmniej: interfejsu, typu ramki Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1p), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP. Urządzenie musi obsługiwać sprzętowo nie mniej niż 8 kolejek per port fizyczny.
19. Urządzenie musi obsługiwać filtrowanie ruchu co najmniej na poziomie portu i sieci VLAN dla kryteriów z warstw 2-4. Urządzenie musi realizować sprzętowo nie mniej niż 7000 reguł filtrowania ruchu. W regułach filtrowania ruchu musi być dostępny mechanizm zliczania dla zaakceptowanych lub zablokowanych pakietów. Musi być dostępna funkcja edycji reguł filtrowania ruchu na samym urządzeniu.
20. Przełącznik musi obsługiwać takie mechanizmu bezpieczeństwa jak limitowanie adresów MAC, Dynamic ARP Inspection, DHCP snooping.
21. Przełącznik musi obsługiwać IEEE 802.1x zarówno dla pojedynczego, jak i wielu suplikantów na porcie. Przełącznik musi przypisywać ustawienia dla użytkownika na podstawie atrybutów zwracanych przez serwer RADIUS (co najmniej VLAN oraz reguła filtrowania ruchu). Musi istnieć

możliwość pominięcia uwierzytelnienia 802.1x dla zdefiniowanych adresów MAC. Przełącznik musi obsługiwać co najmniej następujące typy EAP: MD5, TLS, TTLS, PEAP.

22. Urządzenie musi obsługiwać protokół SNMP (wersje 2c i 3), oraz grupy RMON 1, 2, 3, 9. Musi być dostępna funkcja kopiowania (mirroring) ruchu na poziomie portu i sieci VLAN.
23. Architektura systemu operacyjnego urządzenia musi posiadać budowę modularną (poszczególne moduły muszą działać w odseparowanych obszarach pamięci), m.in. moduł przekazywania pakietów, odpowiedzialny za przełączanie pakietów musi być oddzielony od modułu rutingu IP, odpowiedzialnego za ustalanie tras routingu i zarządzanie urządzeniem.
24. Urządzenie musi posiadać mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 20 poprzednich, kompletnych konfiguracji.

Wymagania gwarancyjne

- Urządzenie powinny być objęte minimum 36 miesięczną gwarancją.

5.5.3 Urządzenie bezpieczeństwa sieciowego ……1 szt.

Wymagania techniczne

- Firewall musi być dostarczony jako dedykowane urządzenie sieciowe o wysokości max. 2 U
- Urządzenie musi być wyposażone w co najmniej 2 GB pamięci RAM, pamięć Flash 2 GB oraz port konsoli. Urządzenie musi posiadać slot USB przeznaczony do podłączenia dodatkowego nośnika danych. Musi być dostępna opcja uruchomienia systemu operacyjnego firewalla z nośnika danych podłączonego do slotu USB na module kontrolnym.
- System operacyjny firewalla musi posiadać budowę modułową (moduły muszą działać w odseparowanych obszarach pamięci) i zapewniać całkowitą separację płaszczyzny kontrolnej od płaszczyzny przetwarzania ruchu użytkowników, m.in. moduł routingu IP, odpowiedzialny za ustalenie tras rutingu i zarządzanie urządzenia musi być oddzielony od modułu przekazywania pakietów, odpowiedzialnego za przełączanie pakietów pomiędzy segmentami sieci obsługiwanymi przez urządzenie. System operacyjny firewalla musi śledzić stan sesji użytkowników (*stateful processing*), tworzyć i zarządzać tablicą stanu sesji. Musi istnieć opcja przełączenia urządzenia w tryb pracy bez śledzenia stanu sesji użytkowników, jak również wyłączenia części ruchu ze śledzenia stanu sesji.
- Urządzenie musi być wyposażone w nie mniej niż 16 wbudowanych interfejsów Ethernet 10/100/1000 (gotowych do użycia bez konieczności zakupu dodatkowych modułów i licencji).
- Urządzenie musi być wyposażone w 4 sloty na dodatkowe karty z modułami interfejsów. Urządzenie musi obsługiwać co najmniej następującej rodzaje kart z modułami interfejsów: ADSL 2/2+, Serial, E1, Gigabit Ethernet (SFP).
- Firewall musi realizować zadania Stateful Firewall z mechanizmami ochrony przed atakami DoS, wykonując kontrolę na poziomie sieci oraz aplikacji pomiędzy nie mniej niż 32 strefami bezpieczeństwa z wydajnością nie mniejszą niż 500 Mb/s liczoną dla ruchu IMIX. Firewall musi przetworzyć nie mniej niż 200 000 pakietów/sekundę (dla pakietów 64-bajtowych). Firewall musi obsłużyć nie mniej niż 128 000 równoległych sesji oraz zestawić nie mniej niż 8 000 nowych połączeń/sekundę.
- Firewall musi zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site. IPSec VPN musi być realizowany sprzętowo. Firewall musi obsługiwać nie mniej niż 1 000 równoległych tuneli VPN oraz ruch szyfrowany o przepustowości nie mniej niż 250 Mb/s. Urządzenie musi posiadać możliwość udostępniania użytkownikom wbudowanego klienta IPSec VPN za pośrednictwem strony WWW.
- Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, użytkowników aplikacji, reakcje zabezpieczeń oraz metody rejestrowania zdarzeń. Firewall musi umożliwiać zdefiniowanie nie mniej niż 4 000 reguł polityki bezpieczeństwa.
- Urządzenie zabezpieczeń musi posiadać funkcję filtrowania zawartości ruchu HTTP, FTP i protokołów poczty elektronicznej (SMTP, POP3, IMAP) w celu blokowania potencjalnie szkodliwych

obiektów. Urządzenie musi filtrować ruch na podstawie kryteriów obejmujących co najmniej: typy MIME, rozszerzenia plików, elementy ActiveX, Java i cookies.

- Urządzenie musi obsługiwać protokoły dynamicznego rutingu: RIP, OSPF oraz BGP. Urządzenie musi umożliwiać skonfigurowanie nie mniej niż 20 wirtualnych routerów.
- Urządzenie musi posiadać możliwość uruchomienia funkcji MPLS z sygnalizacją LDP i RSVP w zakresie VPLS i L3 VPN.
- Urządzenie musi obsługiwać co najmniej 512 sieci VLAN z tagowaniem 802.1Q. W celu zapobiegania zapętlania się ruchu w warstwie 2 firewall musi obsługiwać protokoły Spanning Tree (802.1D), Rapid STP (802.1W) oraz Multiple STP (802.1S). Urządzenie musi obsługiwać protokół LACP w celu agregowania fizycznych połączeń Ethernet.
- Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym QoS – wygładzanie (shaping) oraz obcinanie (policing) ruchu. Mapowanie ruchu do kolejek wyjściowych musi odbywać się na podstawie DSCP, IP ToS, 802.1p, oraz parametrów z nagłówków TCP i UDP. Urządzenie musi posiadać tworzenia osobnych kolejek dla różnych klas ruchu. Urządzenie musi posiadać zaimplementowany mechanizm WRED w celu przeciwdziałania występowaniu przeciążeń w kolejkach.
- Firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie dla urządzeń zabezpieczeń Urządzenia zabezpieczeń w klastrze muszą funkcjonować w trybie Active-Passive z synchronizacją konfiguracji i tablicy stanu sesji. Przełączenie pomiędzy urządzeniami w klastrze HA musi się odbywać przezroczyście dla sesji ruchu użytkowników. Mechanizm ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.
- Zarządzanie urządzeniem musi odbywać się za pomocą graficznej konsoli Web GUI oraz z wiersza linii poleceń (CLI) poprzez port szeregowy oraz protokoły telnet i SSH. Firewall musi posiadać możliwość zarządzania i monitorowania przez centralny system zarządzania i monitorowania pochodzący od tego samego producenta.
- Administratorzy muszą mieć do dyspozycji mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż **5** poprzednich, kompletnych konfiguracji.

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

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

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

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

Wymagania techniczne:
- Moc pozorna 3000VA
- Moc rzeczywista 1800 W
- Architektura UPSa line-interactive
- Maksymalny czas przełączenia na baterię 1,5 ms
- Minimalny czas podtrzymywania dla obciążenia 100% - 6 min
- Minimalny czas podtrzymywania dla obciążenia 50% - 15 min

- Urządzenie powinno posiadać układ automatycznej regulacji napięcia AVR
- Urządzenie powinno być wyposażone w port komunikacyjny RS232
- Urządzenie powinno posiadać oprogramowanie do monitorowania parametrów pracy UPSa
- Możliwość zainstalowania dodatkowego modułu baterii
- Urządzenia powinno posiadać obudowę typu Rack 19''

Wymagania gwarancyjne
- Urządzenie powinno być objęte minimum 36 miesięczną gwarancją.

5.5.6 Serwery i urządzenia dodatkowe

Wymagania techniczne (sprzętowe oraz systemowe):

5.5.6.1 Platforma do wirtualizacji środowisk serwerowych ……..…..1 szt.

LP	Nazwa komponentu	Minimalne wymagania
1	Obudowa	-Typu Rack, wysokość obudowy max.4U (obudowa musi umożliwiać konwersję do obudowy wolnostojącej typu tower); -Dostarczony z szynami montażowymi do szafy rack umożliwiającymi pełne wysunięcie serwera oraz z ramieniem podtrzymującym kable;
2	Płyta główna	-Dwuprocesorowa -Minimum 5 złącz PCI Express Gen.3 w tym minimum 2 złącza o prędkości x16 Gen.3 oraz minimum 1 złącze PCI 32bit; -Możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora (niezależne od dysków twardych);
3	Procesory / Wydajność	-Zainstalowane dwa procesory w architekturze x86 osiągające w oferowanym serwerze w testach wydajności SPECint_rate2006 min. 365 pkt; -Wymagane dołączenie do oferty pełnego protokołu testów SPEC dla oferowanego modelu serwera wyposażonego w oferowane procesory (protokół poświadczony przez Wykonawcę)
4	Pamięć RAM	-Zainstalowane 32 GB pamięci RAM -Wsparcie dla technologii zabezpieczania pamięci Advanced ECC, Memory Scrubbing, SDDC; -Wsparcie dla konfiguracji pamięci w trybie „Rank Sparing"; -12 gniazd pamięci RAM na płycie głównej, obsługa minimum 192GB pamięci RAM;
5	Kontrolery dyskowe, I/O	-Zainstalowany kontroler SAS 2.0 RAID 0,1,5,6,50,60, 512MB pamięci podręcznej cache,
6	Dyski twarde	-Zainstalowane 3 dyski SAS 2.0 o pojemności 600 GB każdy,15K RPM, dyski Hotplug; -Minimum 4 wnęki dla dysków Hotplug w dostarczonej konfiguracji;
7	Inne napędy zintegrowane	-Zintegrowany napęd DVD-RW
8	Kontrolery LAN	-2x 1Gb/s LAN, ze wsparciem iSCSI i iSCSI boot, RJ-45;
9	Porty	-zintegrowana karta graficzna ze złączem VGA; -9x USB 2.0, w tym minimum 2 na panelu przednim i minimum 4 na panelu tylnym; minimum jedno USB 2.0 wewnętrzne umożliwiające instalację pendrive; -1x RS-232;
10	Zasilanie, chłodzenie	-Redundantne zasilacze hotplug o sprawności 94% o mocy maksymalnej 450W;

		-Redundantne wentylatory;
11	Zarządzanie	-Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera – minimum sygnalizacja (poprawna praca/usterka) dla komponentów jak: procesor, wentylatory, dyski twarde, temperatura wewnątrz obudowy, pamięci, zasilaczy; sygnalizacja pracy (zasilania), sygnalizacja identyfikacji (włączana zdalnie) -Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; • Dedykowana karta LAN 1 Gb/s RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; • Dodatkowe złącze serwisowe RJ-45 1Gb/s dostępne z przodu obudowy • Dostęp poprzez przeglądarkę Web (także SSL, SSH) • Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii • Zarządzanie alarmami (zdarzenia poprzez SNMP) • Możliwość przejęcia konsoli tekstowej • Możliwość przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) • Oprogramowanie zarządzające i diagnostyczne umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.).
12	Wspierane systemy operacyjne	Wymagana jest współpraca z systemami oferowanymi przez Wykonawcę do realizacji zamówienia
13	Gwarancja	- co najmniej 3 lata gwarancji , serwis w miejscu instalacji sprzętu, - Czas reakcji na zgłoszenie serwisowe - w następny dzień roboczy po otrzymaniu zgłoszenia. -Dostępność części zamiennych przez 5 lat od momentu zakupu serwera;
14	Dokumentacja, inne	- Serwer musi być fabrycznie nowy - Wykonawca zobowiązany jest dostarczyć wraz z ofertą kartę produktową oferowanego serwera umożliwiającą weryfikację parametrów oferowanego sprzętu; - Ogólnopolska, telefoniczna infolinia/linia techniczna, (ogólnopolski numer o zredukowanej odpłatności 0-800/0-801, w ofercie należy podać nr telefonu) w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; -Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera lub Wykonawcy ;
15	Zainstalowany system operacyjny	System operacyjny zainstalowany na dostarczonym serwerze posiadający następujące funkcjonalności: • Licencja na oprogramowanie musi być przypisana do każdego procesora fizycznego serwera.

		• Liczba rdzeni procesorów i ilość pamięci nie mogą mieć wpływu na liczbę wymaganych licencji. • Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. • Możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym • Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny. • Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania min. 8000 maszyn wirtualnych. • Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. • Wsparcie dodawania i wymiany pamięci RAM bez przerywania pracy. • Wsparcie dodawania i wymiany procesorów bez przerywania pracy. • Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. • Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading lub równoważne. • Wbudowane wsparcie instalacji i pracy na wolumenach, które: a. pozwalają na zmianę rozmiaru w czasie pracy systemu, b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) wgląd w poprzednie wersje plików i folderów, c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d. umożliwiają zdefiniowanie list kontroli dostępu. e. Wbudowany mechanizm klasyfikowania i indeksowania plików w oparciu o ich zawartość. f. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny tj. wydany przez agendę rządową zajmującą się bezpieczeństwem informacji. g. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów h. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. i. Graficzny interfejs użytkownika. j. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, k. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji l. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). m. Możliwość zdalnej konfiguracj i, administrowania oraz aktualizowania systemu. n. Dostępność bezpłatnych narzędzi umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. o. Serwis zarządzania polityką konsumpcji informacji w dokumentach

		(Digital Rights Management). p. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: - Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, - Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, - Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. - Zdalna dystrybucja oprogramowania na stacje robocze. c. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej d. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: - Dystrybucję certyfikatów poprzez http - Konsolidację CA dla wielu lasów domeny, - Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.Szyfrowanie plików i folderów. e. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). f. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. g. Serwis udostępniania stron WWW. h. Wsparcie dla protokołu IP w wersji 6 (IPv6), i. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach, j. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. k. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności l. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: - Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, - Obsługi ramek typu jumbo frames dla maszyn wirtualnych. - Obsługi 4-KB sektorów dysków - Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra - Wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku różnych dostawców poprzez otwarty interfejs API. - Kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model) m. Możliwość automatycznej aktualizacji w oparciu o poprawki

		publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. n. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). o. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. p. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. q. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management. r. Materiały edukacyjne w języku polskim.

Wymagania ogólne dotyczące instalacji oprogramowania na serwerze:

Na dostarczonym serwerze należy zainstalować oraz skonfigurować następujące oprogramowanie:

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

a) System monitoringu infrastruktury sieciowej (1 kpl.)

Wymagania funkcjonalne systemu monitoringu stanu sieci:

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

1. System zarządzania bezpieczeństwem musi utrzymywać centralne repozytorium logów pobieranych z innych urządzeń i systemów oraz realizować funkcje Security Information and Event Management (SIEM) i Network Behavior Anomalny Detection (NBAD).
2. Moduł SIEM musi pobierać logi z wielu różnych elementów systemu informatycznego, poddawać je korelacji i na tej podstawie przedstawiać administratorom wiarygodne informacje na temat stanu bezpieczeństwa i wykrytych incydentów.
3. Moduł NBAD na podstawie statystyk i opisu ruchu (NetFlow, itp.) pobieranych bezpośrednio z urządzeń sieciowych (ruterów, przełączników) musi dokonywać

analizy stanu i efektywności pracy sieci, w tym wykrywania sytuacji nieprawidłowych (anomalii).

4. Moduł NBAD musi dokonywać wykrywania anomalii w systemie informatycznym za pomocą analizy behawioralnej. W tym celu muszą być na bieżąco budowane profile normalnego stanu i zachowania sieci oraz identyfikowane odchylenia (m.in. zmiany stanu, nagłe zwiększenia lub zmniejszenia natężenia ruchu i przekroczenie wartości progowych).
5. Moduł NBAD musi posiadać możliwość wykrywania nowych obiektów w systemie informatycznym (hostów, aplikacji, protokołów, itd.). Moduł NBAD musi także posiadać możliwość wykrywania awarii systemów, m.in. zablokowanych lub uszkodzonych serwerów i aplikacji.
6. System zarządzania musi być dostarczony jako jedno, gotowe do użycia urządzenia (appliance). Nie jest dopuszczalne oprogramowanie instalowane na sprzęcie ogólnego przeznaczenia.
7. Urządzenie Appliance musi posiadać minimum 8 GB pamięci RAM oraz 2 dyski o pojemności co najmniej 500 GB funkcjonujących w konfiguracji RAID 1.
8. Urządzenie Appliance musi posiadać wydajność co najmniej 250 zdarzeń na sekundę oraz 7 500 strumieni (Flows) na minutę.
9. Urządzenie Appliance musi działać na bazie dostrojonego przez producenta systemu operacyjnego klasy Linux. Nie jest dopuszczalne zastosowanie do tego celu systemu operacyjnego Microsoft Windows.
10. Urządzenie Appliance musi umożliwiać integrację z zewnętrznymi repozytoriami danych, co najmniej iSCSI SAN i NAS.
11. Wszystkie funkcje systemu (SIEM, NBAD) muszą być dostępne są w ramach jednego urządzenia Appliance.
12. Moduły SIEM i NBAD muszą być zintegrowane ze sobą tak, aby informacje o naruszeniach bezpieczeństwa były przedstawiane na podstawie analiz obu tych modułów.
13. Obsługa incydentów bezpieczeństwa musi odbywać się na podstawie wielu źródeł informacji, nie mniej niż:

– zdarzenia i logi z systemów zabezpieczeń (firewall, VPN, IPS, AV, itd.), systemów operacyjnych (Unix, Microsoft Windows, itd.) oraz aplikacji i baz danych,
– statystyki i opis ruchu sieciowego odbierane z urządzeń za pomocą NetFlow, J-Flow, S-Flow i Bluecoat Packetshaper oraz odczytywane bezpośrednio z sieci (span port),
– informacje na temat stanu systemów i ich słabości bezpieczeństwa odczytywane za pomocą Juniper IDP Profiler oraz skanerów Nessus, NMAP, nCircle i Qualys.

14. System zarządzania musi umożliwiać pobieranie logów z innych systemów za pomocą wielu metod, nie mniej niż Syslog (standardowy format logów, protokoły TCP i UDP), SNMP (wiadomości o zdarzeniach przesyłane poprzez SNMP Trap), a także Security Device Event Exchange (SDEE) i Java Database Connectivity API (JDBC).
15. System zarządzania musi umożliwiać odczytywanie logów z systemów operacyjnych Microsoft Windows i Unix, nie mniej niż Redhat Linux, IBM AIX i SUN Solaris.
16. System zarządzania w zakresie odczytu logów musi umożliwiać integrację z innymi systemami zarządzania zabezpieczeń, nie mniej niż Juniper Network and Security Manager, IBM ISS SiteProtector i Check Point SmartCenter.
17. Administratorzy bezpieczeństwa muszą mieć do dyspozycji dedykowane, graficzne narzędzia, uruchamiane z wykorzystaniem standardowej przeglądarki Web. Nie jest dopuszczalne instalowanie do tego celu dodatkowych aplikacji.
18. System zarządzania musi posiadać możliwość powiadamiania administratorów o zdarzeniach za pomocą co najmniej email, SNMP oraz Syslog. System zarządzania musi posiadać możliwość nawiązania połączenia z urządzeniami zabezpieczeń sieci w celu zablokowania niedozwolonej komunikacji.
19. System zarządzania musi umożliwiać przypisywanie zidentyfikowanych incydentów bezpieczeństwa do obsługi określonym administratorom.

20. System zarządzania musi umożliwiać wdrożenie w architekturze scentralizowanej (wszystkie funkcje na jednym Appliance) oraz rozproszonej, złożonej z wielu urządzeń. Struktura rozproszona budowana jest w celu zwiększenia wydajności systemu. W przypadku rozproszonej struktury zarządzanie całości systemu musi odbywać się z jednej konsoli. W przypadku rozproszonej struktury musi być możliwość kryptograficznej ochrony (szyfrowanie) komunikacji sieciowej pomiędzy komponentami systemu.
21. System zarządzania musi umożliwiać definiowanie precyzyjnych uprawnień administratorów w zakresie monitorowanego obszaru systemu informatycznego oraz dostępnych operacji w systemie zarządzania. Tożsamość administratorów musi być weryfikowana poprzez lokalne konto oraz zewnętrzne systemy uwierzytelniania - co najmniej RADIUS, LDAP i Active Directory.
22. System zarządzania do celów obsługi zdarzeń musi utrzymywać centralne repozytorium logów z możliwością ich przeglądania w formie rzeczywistej (raw) oraz znormalizowanej. Dla logów system musi utrzymywać wskaźniki czasu (time stamp). Starsze logi muszą być poddawane kompresji.
23. System zarządzania musi składować informacje w bazie danych zaprojektowanej do tego celu przez producenta. Nie jest dopuszczalne użycie do tego celu bazy danych ogólnego przeznaczania.
24. Składowane w systemie zarządzania informacje muszą być zabezpieczone kryptograficznie za pomocą sum kontrolnych - dostępne są minimum funkcje MD2, MD5, SHA-1 oraz SHA-2 (NIST FIPS 180-2).
25. System zarządzania musi mieć możliwość wykonywania operacji backup i restore, uruchamianych z graficznej konsoli. System zarządzania musi mieć możliwość wykonywania archiwizacji informacji do zewnętrznych repozytoriów danych – nie mniej niż iSCSI SAN i NAS.
26. System zarządzania musi posiadać możliwość tworzenia wielu typów raportów generowanych zgodnie z kryteriami ustalonymi przez administratorów oraz na podstawie predefiniowanych wzorców (raportów). Raporty muszą być tworzone są w wielu formatach - minimum PDF, HTML, CSV, RTF i XML.
27. System zarządzania musi posiadać co najmniej 200 predefiniowanych raportów. W celu sprawnego przeszukiwania predefiniowanych raportów muszą być one pogrupowane - co najmniej według typu urządzeń i zdarzeń bezpieczeństwa. W systemie muszą być dostępne predefiniowane raporty na zgodność ze standardami bezpieczeństwa - minimum dla PCI i SOX.
28. System zarządzania musi utrzymywać szczegółowy log audytowy rejestrujący co najmniej następujące operacje administratorów - login/logoff i zmiany konfiguracji systemu.
29. System zarządzania musi posiadać możliwości weryfikacji poprawności swojego działania i powiadamiania administratorów o nieprawidłowościach - co najmniej za pomocą wpisu do logów systemowych oraz SNMP Trap.

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

Wymagania funkcjonalne systemu LMS:

Wymagana jest dostawa oraz konfiguracja specjalizowanego oprogramowania (wraz z wszelkimi niezbędnymi licencjami) tworzącego system zarządzania oraz administracji usługami dostępu do Internetu oraz użytkownikami sieci.
System ten powinien cechować się następującą funkcjonalnością:

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

- przyjazny intuicyjny graficzny interfejs zrealizowany w technologii WWW - udostępniony w sieci zarządzania poprzez protokół http/https
- zarządzanie dostępem do usług (w tym kontrola pasma i statystyk, możliwość prostego włączenia/wyłączenia dostępu do usługi) – tworzenie taryf z definicja parametrów upload/download, ilość połączeń na sekundę, limit danych
- współpraca z zaproponowanym systemem „TrafficManager" – generowanie kolejkowania ruchu w oparciu o zdefiniowane w bazie usługi oraz „klientów" sieci
- ewidencja sprzętu sieciowego – urządzeń sieci (nazwa, model, producent, numer seryjny, hasła dostępu, data zakupu, okres gwarancji, ilość portów, lokalizacja, itp.) oraz urządzeń dostępowych klienta
- ewidencja adresacji sieci – ip, mac
- inwentaryzacja połączeń urządzeń sieciowych, tworzenie powiązań z urządzeniami klienckimi podłączonymi do urządzeń dostępowych oraz możliwość graficznej prezentacji tak zdefiniowanych połączeń
- przechowywanie danych klientów, konfiguracja usługi, przechowywanie informacji o urządzeniach dostępowych klienta, generowanie oraz przetrzymywanie dokumentów klienta (np. umowa, 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 role bramy dla klienckich sieci dostępowych oraz nakładającego na ruch wychodzący oraz wchodzący z Internetu odpowiednie polityki kształtowania ruchu zgodnie ze zdefiniowanymi w systemie LMS usługami oraz stacjami końcowymi.

Oprogramowanie musi posiadać następujące cechy i funkcje:

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

P2P)
5. generowanie klas ruchu dla aktywnych klientów z bazy LMS
6. limitowanie ilości połączeń użytkownika sieci – zgodnie z definicja taryfy w systemie LMS
7. możliwość ustalenia różnych limitów na dzień/noc
8. limitowanie wielkości transferu dla dowolnego okresu czasu

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

5.5.6.2 Dostawa i instalacja systemu pamięci masowej ……**1 szt**

Nazwa komponentu	Wymagane minimalne parametry techniczne
System operacyjny	dedykowany, typu embedded
Procesor	klasy x86, dedykowany do pracy w systemach pamięci masowej uzyskujący przy pracy w nominalnych warunkach w teście Passmark CPU Mark wynik min. 800 punktów (wynik zaproponowanego procesora musi znajdować się na stronie http://www.cpubenchmark.net, z której wydruk należy dołączyć do oferty)
Pamięć	nieulotna 512 MB typu Flash, operacyjna 1 GB
System dyskowy	- dostępne 8 kieszeni 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, 6+ hot spare JBOD - system plików ext3, ext4 (dyski wewnętrzne), ext3, ext4, NTFS, FAT32, HFS+ (dyski zewnętrzne)
Interfejsy	- 2 x Gigabit Ethernet z obsługą iSCSI - 4 x USB 2.0 - 2 x eSATA
Obudowa	- wysokość max. 3U ,dedykowana do montażu w szafie rack 19" z zestawem szyn mocujących - dwa zasilacze redundantne - przyciski: Power, USB One-Touch-Backup, reset - wyświetlacz LCD
Wspierane systemy operacyjne	Wymagana jest współpraca z systemami oferowanymi przez Wykonawcę do realizacji zamówienia
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, zarządzanie kontami użytkowników (maksymalnie 4096 użytkowników), zarządzanie grupą użytkowników (maksymalnie 512 grup), tworzenie zestawów użytkowników
Dodatkowe oprogramowanie	oprogramowanie do tworzenia obrazów dysku, przywracania systemu od podstaw, szybkiego odzyskiwania bez konieczności ponownego instalowania systemu operacyjnego i aplikacji, zawierające: - rozbudowane funkcje katalogowania do łatwego przeglądania, wyszukiwania i przywracania różnych wersji poszczególnych plików z kopii zapasowych obrazów - szybkie, jednoczesne, bez agentowe operacje tworzenia kopii zapasowych i odzyskiwania maszyn wirtualnych - możliwość tworzenia kopii zapasowych i odzyskiwania danych na nieograniczonej liczbie maszyn wirtualnych działających na hoście, a także wykonywanie migracji typu V2P i P2V . Ilość licencji: 2
Gwarancja	- Gwarancja co najmniej 36 miesięcy. - Czas reakcji serwisu w następnym dniu roboczym po zgłoszeniu - W przypadku awarii urządzenia , Zamawiającemu musi zostać dostarczone urządzenia zastępcze na czas naprawy. - wsparcie techniczne w przypadku problemów ze współpracą z innymi elementami sieci, - asysta telefoniczna / e-mailowa przy aktualizacji oprogramowania, - pomoc techniczna w sprawach nietypowych, modyfikacjach oprogramowania itp.

5.5.6.3 Stacja do zarządzania …….…….. **1 szt.**

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
1	Zastosowanie	Komputer przenośny będzie wykorzystywany dla potrzeb zarządzania siecią szerokopasmową
2	Przekątna ekranu	Komputer przenośny typu notebook z ekranem 15,6" o rozdzielczości HD (1366 x 768) z podświetleniem LED
3	Wydajność	Oferowany komputer musi osiągać w teście wydajnościowym PCMark Vantage Profesional Edition z zainstalowaną poprawką 102 przy standardowych ustawieniach oprogramowania testującego: - PCMark Score – minimum 5300 punktów, - Communications Score – minimum 7100 punktów - Productivity Score – minimum 4950 punktów Dokumentem potwierdzającym spełnianie ww. wymagań będzie dołączony do oferty wydruk raportu z oprogramowania testującego lub wydruk zawartości ekranu [Print Screen ekranu] z przeprowadzonych testów, potwierdzony za zgodność z oryginałem przez Wykonawcę. Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testu Wykonawca może zostać wezwany do dostarczenia Zamawiającemu oprogramowania testującego, komputera do testów oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 5 dni od otrzymania zawiadomienia od Zamawiającego
4	Płyta główna	Wyposażona w dedykowany chipset dla oferowanego procesora.
5	Pamięć RAM	4GB z możliwością rozbudowy do min 8GB, jeden slot wolny
6	Pamięć masowa	500 GB
7	Karta graficzna	Obsługująca rozdzielczość zintegrowanego ekranu LCD.
8	Napęd optyczny	Nagrywarka DVD-RW

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
9.	Klawiatura	Klawiatura z powłoką antybakteryjną (układ US -QWERTY),
10	Multimedia	Dwukanałowa (24-bitowa) karta dźwiękowa, zgodna z High Definition,
11	Bateria i zasilanie	Min. 40WHr Zasilacz o mocy min. 65W
12	Waga	Waga max 2,5 kg z baterią
13	Obudowa	Obudowa notebooka wzmocniona, szkielet i zawiasy notebooka wykonany z metalu.
14	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu).
15	BIOS	BIOS zgodny ze specyfikacją UEFI Możliwość, bez uruchamiania systemu operacyjnego odczytania z BIOS informacji o: – wersji BIOS, – nr seryjnym komputera wraz z datą jego wyprodukowania, – ilości i sposobu obłożenia slotów pamięciami RAM, – typie procesora wraz z informacją o ilości rdzeni, wielkości pamięci cache L2 i L3, – pojemności zainstalowanego dysku twardego – MAC adresie zintegrowanej karty sieciowej – zainstalowanej grafice – typie panelu LCD wraz z informacją o jego natywnej rozdzielczości – kontrolerze audio Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z USB Możliwość, bez uruchamiania systemu operacyjnego, ustawienia hasła na poziomie systemu, administratora oraz dysku twardego oraz możliwość ustawienia następujących zależności pomiędzy nimi: brak możliwości zmiany hasła pozwalającego na uruchomienie systemu bez podania hasła administratora. Musi posiadać możliwość ustawienia zależności pomiędzy hasłem administratora a hasłem systemowym tak, aby nie było możliwe wprowadzenie zmian w BIOS wyłącznie po podaniu hasła systemowego. Funkcja ta ma wymuszać podanie hasła administratora przy próbie zmiany ustawień BIOS w sytuacji, gdy zostało podane hasło systemowe. Możliwość wyłączenia/włączenia: zintegrowanej karty sieciowej, portów USB, czytnika kard multimedialnych, mikrofonu, kamery, pracy wielordzeniowej procesora, modułów: WWAN, WLAN i Bluetooth z poziomu BIOS, bez uruchamiania systemu operacyjnego. Możliwość włączenia/wyłączenia funkcjonalności Wake On LAN/WLAN – zdalne uruchomienie komputera za pośrednictwem sieci LAN i WLAN – min. trzy opcje do wyboru: tylko LAN, tylko WLAN, LAN oraz WLAN Możliwość włączenia/wyłączenia hasła dla dysku twardego Możliwość przypisania w BIOS numeru nadawanego przez Administratora/Użytkownika oraz możliwość weryfikacji tego numeru w oprogramowaniu diagnostyczno-zarządzającym producenta komputera.
16	Certyfikaty	- certyfikat ISO9001 lub równoważny dla producenta urządzenia - EnergyStar 5.0 - Deklaracja zgodności CE
17	Zgodność z systemami operacyjnymi i standardami	Należy załączyć wydruk ze strony www producenta oprogramowania potwierdzający poprawną współpracę oferowanych modeli komputerów z oferowanym systemem operacyjnym lub oświadczenie Wykonawcy

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
18	Zainstalowane oprogramowanie	Zainstalowany **system operacyjny,** wraz z nośnikiem i przeglądarką internetową w polskiej wersji językowej, niewymagający wpisywania klucza rejestracyjnego lub rejestracji poprzez Internet czy telefon, musi spełniać następujące wymagania: 1. Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek. 2. Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet. 3. Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) 4. Internetowa aktualizacja zapewniona w języku polskim. 5. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 6. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe. 7. Wsparcie dla powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug &Play, Wi-Fi). 8. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer. 9. Interfejs użytkownika działający w trybie graficznym, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta 10. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu 11. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 12. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z co najmniej: poziomu menu, poziomu otwartego okna systemu operacyjnego 13. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. 14. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. 15. Wbudowany system pomocy w języku polskim. 16. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 17. Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji. 18. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. 19. Wsparcie dla logowania przy pomocy smartcard. 20. Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji. 21. System musi posiadać narzędzia służące do administracji, wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk. 22. Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 lub programów równoważnych, tj. – umożliwiających uruchomienie aplikacji działających we wskazanych środowiskach. 23. Wsparcie dla JScript i VBScript lub równoważnych – możliwość uruchamiania interpretera poleceń. 24. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 25. Rozwiązanie służące do automatycznego zbudowania obrazu

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
		systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową. 26. Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację. 27. Graficzne środowisko instalacji i konfiguracji. 28. Transakcyjny system plików pozwalający na stosowanie przydziałów na dysku dla użytkowników i pozwalający tworzyć kopie zapasowe. 29. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. 30. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 31. Możliwość przywracania plików systemowych. 32. Możliwość identyfikacji sieci komputerowych, do których jest podłączony komputer, zapamiętywania ustawień i przypisywania do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 33. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). Zainstalowane **oprogramowanie biurowe** - kompletny pakiet oprogramowania biurowego musi spełniać następujące wymagania: 1. Wymagania odnośnie interfejsu użytkownika: • pełna polska wersja językowa interfejsu użytkownika • prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych • możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się. 2. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: a) posiada kompletny i publicznie dostępny opis formatu, b) ma zdefiniowany układ informacji w postaci XML zgodnie z Tabelą B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766) c) umożliwia wykorzystanie schematów XML d) obsługuje w ramach standardu formatu podpis elektroniczny zgodnie z Tabelą A.1.1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766) 3. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców. 4. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy)

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
		5. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim. 6. Pakiet zintegrowanych aplikacji biurowych musi zawierać: a) edytor tekstów b) arkusz kalkulacyjny c) narzędzie do przygotowywania i prowadzenia prezentacji d) narzędzie do tworzenia i wypełniania formularzy elektronicznych e) narzędzie do tworzenia drukowanych materiałów informacyjnych f) narzędzie do tworzenia i pracy z lokalną bazą danych g) narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) 7. <u>Edytor tekstów musi umożliwiać:</u> a) Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty; b) wstawianie oraz formatowanie tabel; c) wstawianie oraz formatowanie obiektów graficznych; d) wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne); e) automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków; a f) automatyczne tworzenie spisów treści; g) formatowanie nagłówków i stopek stron; h) sprawdzanie pisowni w języku polskim; i) śledzenie zmian wprowadzonych przez użytkowników; j) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności; k) określenie układu strony (pionowa/pozioma); l) wydruk dokumentów; m) wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną; n) pracę na dokumentach utworzonych przy pomocy MS Word 2003 lub 2007 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu; zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji 8. <u>Arkusz kalkulacyjny musi umożliwiać:</u> a) Tworzenie raportów tabelarycznych; b) tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych; c) tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu; d) tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice); e) obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych; f) tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych; g) wyszukiwanie i zamianę danych; wykonywanie analiz danych przy użyciu formatowania warunkowego; h) nazywanie komórek arkusza i odwoływanie się w formułach po

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
		takiej nazwie; i) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności; j) formatowanie czasu, daty i wartości finansowych z polskim formatem; k) zapis wielu arkuszy kalkulacyjnych w jednym pliku; l) zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania MS Excel 2003 i 2007, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń; m) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji 9. <u>Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:</u> a) Przygotowywanie prezentacji multimedialnych, które będą: • prezentowane przy użyciu projektora multimedialnego; • drukowane w formacie umożliwiającym robienie notatek; • zapisane jako prezentacja tylko do odczytu; b) nagrywanie narracji i dołączanie jej do prezentacji; c) opatrywanie slajdów notatkami dla prezentera; d) umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo; e) umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego; f) odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym; g) możliwość tworzenia animacji obiektów i całych slajdów; h) prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, i) pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003 i 2007. 10. <u>Narzędzie do tworzenia i wypełniania formularzy elektronicznych musi umożliwiać:</u> a) Przygotowanie formularza elektronicznego i zapisanie go w pliku w formacie XML bez konieczności programowania; b) umieszczenie w formularzu elektronicznym pól tekstowych, wyboru, daty, list rozwijanych, tabel zawierających powtarzające się zestawy pól do wypełnienia oraz przycisków; c) utworzenie w obrębie jednego formularza z jednym zestawem danych kilku widoków z różnym zestawem elementów, dostępnych dla różnych użytkowników; d) pobieranie danych do formularza elektronicznego z plików XML lub z lokalnej bazy danych wchodzącej w skład pakietu narzędzi biurowych; e) możliwość pobierania danych z platformy do pracy grupowej; f) przesłanie danych przy użyciu usługi Web (tzw. webservice); g) wypełnianie formularza elektronicznego i zapisywanie powstałego w ten sposób dokumentu w pliku w formacie XML; h) podpis elektroniczny formularza elektronicznego i dokumentu powstałego z jego wypełnienia 11. <u>Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać:</u> a) Tworzenie i edycję drukowanych materiałów informacyjnych; b) tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów; c) edycję poszczególnych stron materiałów; d) podział treści na kolumny;

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
		e) umieszczanie elementów graficznych; f) wykorzystanie mechanizmu korespondencji seryjnej; g) płynne przesuwanie elementów po całej stronie publikacji; h) eksport publikacji do formatu PDF oraz TIFF; i) wydruk publikacji; możliwość przygotowywania materiałów do wydruku w standardzie CMYK 12. Narzędzie do tworzenia i pracy z lokalną bazą danych musi umożliwiać: a) Tworzenie bazy danych przez zdefiniowanie: • tabel składających się z unikatowego klucza i pól różnych typów, w tym tekstowych i liczbowych • relacji pomiędzy tabelami; • formularzy do wprowadzania i edycji danych; • raportów; b) edycję danych i zapisywanie ich w lokalnie przechowywanej bazie danych; c) tworzenie bazy danych przy użyciu zdefiniowanych szablonów; d) połączenie z danymi zewnętrznymi, a w szczególności z innymi bazami danych zgodnymi z ODBC, plikami XML, arkuszem kalkulacyjnym 13. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: a) Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego; b) filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców; c) tworzenie katalogów, pozwalających katalogować pocztę elektroniczną; d) tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy; e) oflagowanie poczty elektronicznej z określeniem terminu przypomnienia; f) zarządzanie kalendarzem; g) udostępnianie kalendarza innym użytkownikom; h) przeglądanie kalendarza innych użytkowników; i) zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach; j) zarządzanie listą zadań; k) zlecanie zadań innym użytkownikom; l) zarządzanie listą kontaktów; m) udostępnianie listy kontaktów innym użytkownikom; n) przeglądanie listy kontaktów innych użytkowników; o) możliwość przesyłania kontaktów innym użytkownikom. Zainstalowany **program antywirusowy** musi spełniać następujące wymagania: 1. Pełne wsparcie dla oferowanego systemu operacyjnego w wersji 64 bitowej. 2. Interfejsy programu, pomoce i podręczniki w języku polskim. 3. Pomoc techniczna w języku polskim. 4. Multijęzyczny instalator – przynajmniej 5 wersji językowych. 5. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 6. Wykrywanie i usuwanie niebezpiecznych programów: adware,

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
		spyware, scareware, phishing, hacktools itp. 7. Wbudowana technologia do ochrony przed rootkitami wykrywająca aktywne i nieaktywne rootkity. 8. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 9. Min. 2 niezależne skanery antywirusowe z 2 niezależnymi bazami sygnatur wirusów wykorzystywane przez skaner dostępowy, skaner na żądanie oraz skaner poczty elektronicznej. 10. Możliwość konfiguracji programu do pracy z jednym (dowolnym) skanerem antywirusowym lub dwoma skanerami antywirusowymi jednocześnie. 11. Technologia kontroli zachowania aplikacji. 12. Kontrola rejestru i pliku autostartu. 13. Kontrola autostartu – możliwość opóźnienia uruchamiania aplikacji z autostartu podczas startu systemu. 14. Skanowanie w trybie bezczynności – pełne skanowanie komputera min. raz na 2 tygodnie uruchamiane i wznawiane automatycznie, podczas gdy nie jest używany. 15. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików na żądanie lub według harmonogramu. 16. 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). 17. Wykrywanie obecności zasilania bateryjnego przed uruchamianiem skanowania. 18. Skanowanie na żądanie pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 19. Możliwość min. 3-stopniowej regulacji obciążenia generowanego przez program 20. Możliwość eksportowania i importowania ustawień programu. 21. Możliwość zabezpieczenia ustawień programu hasłem. 22. Możliwość określania poziomu obciążenia procesora podczas skanowania na żądanie i według harmonogramu. 23. Możliwość wyłączenia komputera po zaplanowanym skanowaniu jeśli żaden użytkownik nie jest zalogowany. 24. Możliwość skanowania dysków sieciowych i dysków przenośnych. 25. Rozpoznawanie i skanowanie wszystkich znanych formatów kompresji. 26. Możliwość definiowania listy plików, folderów i napędów pomijanych przez skaner dostępowy. 27. 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. 28. Dedykowany moduł ochrony bankowości internetowej, nie bazujący na bazach sygnatur wirusów jak i analizie heurystycznej (heurystyce). Moduł ten ma współpracować z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 29. Skanowanie i oczyszczanie poczty przychodzącej POP3 w czasie rzeczywistym, zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
		klienta pocztowego). 30. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. 31. Możliwość definiowania różnych portów dla POP3, SMTP i IMAP na których ma odbywać się skanowanie. 32. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. 33. Skanowanie ruchu HTTP. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. 34. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 35. Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie. 36. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. 37. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń powinny być w pełni anonimowe. 38. Aktualizacja dostępna z bezpośrednio Internetu, lub offline – z pliku pobranego zewnętrznie. 39. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. 40. Możliwość określenia częstotliwości aktualizacji w odstępach min. 1 godzinowych. 41. Program wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, antyspam, skaner HTTP). 42. Raportowanie wykrytych zagrożeń i wszystkich przeprowadzonych działań. 43. Kreator płyt startowych umożliwiających nagrywanie płyt skanujących komputer bez udziału systemu operacyjnego. 44. Kreator musi nagrywać obraz płyty bezpośrednio na nośnik CD lub zapisać go na dysku. 45. System operacyjny wykorzystywany przez płytę startową musi umożliwiać uaktualnienie sygnatur wirusów przez Internet przed rozpoczęciem skanowania. 46. System operacyjny wykorzystywany przez płytę startową musi automatycznie wykrywać sieci bezprzewodowe. 47. Interfejs programu musi informować o terminie ważności licencji. 48. Program musi wyświetlać monity o zbliżającym się zakończeniu licencji, a także powiadamiać o zakończeniu licencji. 49. Użytkownik musi mieć możliwość podejrzenia numeru rejestracyjnego zastosowanego w programie. Prawo do bezpłatnej aktualizacji baz wirusów i innych zagrożeń przez okres 3 lat od dnia odbioru przez Zamawiającego
19	Diagnostyka	Wbudowany wizualny system diagnostyczny oparty na sygnalizacji za pomocą diod umożliwiający wykrycie bez konieczności uruchamiania systemu operacyjnego min.: awarię procesora, błędy pamięci, awarię płyty głównej, awarię karty graficznej, braku pamięci, problemu z panelem LCD, problemu z ukończeniem procesu systemu POST, problemu z zainicjowaniem/obsługą pamięci
20	Porty i złącza	– Wbudowane porty i złącza : VGA, RJ-45 (10/100/1000), 2x USB 3.0, 2x USB 2.0, czytnik kart multimedialny wspierający min. karty

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
		SD i SDHC 4.0, złącze słuchawkowe stereo i złącze mikrofonowe (dopuszcza się złącze współdzielone) – Zintegrowana w postaci wewnętrznego modułu mini-PCI Express karta sieci WLAN obsługująca łącznie standardy IEEE 802.11 b/g/n – Moduł bluetooth 4.0 – Touchpad z strefą przewijania w pionie, poziomie wraz z obsługą gestów
22	Warunki gwarancji	5-letnia gwarancja świadczona na miejscu u klienta, czas reakcji serwisu - do końca następnego dnia roboczego - Serwis gwarancyjny musi być świadczony przez producenta komputera, jego autoryzowanego partnera serwisowego lub Wykonawcę

5.6 Dostawa, instalacja sprzętu komputerowego i oprogramowania

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

5.6.1 Dostawa zestawów komputerowych wraz z podstawowym oprogramowaniem z przeznaczeniem dla beneficjentów ostatecznych – 200 kpl

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
1	Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych
2	Typ	Komputer stacjonarny. W ofercie wymagane jest dołączenie karty katalogowej
3	Procesor	Procesor klasy x86, zaprojektowany do pracy w komputerach stacjonarnych, osiągający w teście PassMark CPU Mark wynik min. 3050 punktów (wynik zaproponowanego procesora musi znajdować się na stronie http://www.cpubenchmark.net, z której wydruk należy dołączyć do oferty) Ponadto oferowany komputer musi osiągać w testach wydajności wyniki nie niższe niż: PCMark Vantage Profesional Edition z zainstalowaną poprawką 102 przy standardowych ustawieniach oprogramowania testującego: - PCMark Score – minimum 6380 punktów, - Communications Score – minimum 7450 punktów - Productivity Score – minimum 5400 punktów

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
		Test powinien być przeprowadzony przy rozdzielczości standardowej dla oprogramowania testującego Dokumentem potwierdzającym spełnianie ww. wymagań będzie dołączony do oferty wydruk raportu z oprogramowania testującego lub wydruk zawartości ekranu [Print Screen ekranu] z przeprowadzonych testów, potwierdzony za zgodność przez Wykonawcę. Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testu Wykonawca może zostać wezwany do dostarczenia Zamawiającemu oprogramowania testującego, komputera do testów oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 5 dni od otrzymania zawiadomienia od Zamawiającego
4	Pamięć operacyjna	4GB, możliwość rozbudowy do min 16GB, min. trzy sloty wolne
5	Dysk twardy	Min. 500 GB
6	Karta graficzna	Grafika powinna umożliwiać pracę dwumonitorową ze wsparciem dla HDMI v1.4 z 3D, ze sprzętowym wsparciem dla kodowania H.264 oraz MPEG2, DirectX 11, OpenGL 3.0, Shader 4.1
7	Wyposażenie multimedialne	Min 24-bitowa Karta dźwiękowa, zgodna z High Definition, porty słuchawek i mikrofonu na przednim oraz na tylnym panelu obudowy.
8	Obudowa i zasilacz	Małogabarytowa typu small form factor, z obsługą kart PCI Express o niskim profilu, fabrycznie przystosowana do pracy w układzie pionowym i poziomym wyposażona w min. 2 kieszenie: 1 szt 5,25” zewnętrzne typu i 1 szt 3,5” wewnętrzne, Obudowa powinna fabrycznie umożliwiać montaż min 1 szt. dysku 3,5” lub 2 szt. dysków 2,5” Zasilacz o mocy max 240W pracujący w sieci 230V 50/60Hz prądu zmiennego Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych) Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) oraz kłódki (oczko w obudowie do założenia kłódki). Obudowa musi posiadać wbudowany wizualny i dźwiękowy system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, a w szczególności musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie złączy PCI i PCIe, płyty głównej, uszkodzenie kontrolera video, uszkodzenie dysku twardego, awarię BIOS’u, awarię procesora. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów wymaganych dla płyty głównej
9	Zgodność z systemami operacyjnymi i standardami	Należy załączyć wydruk ze strony www producenta oprogramowania potwierdzający poprawną współpracę oferowanych modeli komputerów z oferowanym systemem operacyjnym lub oświadczenie Wykonawcy
10	Bezpieczeństwo	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
11	Zdalne zarządzanie	Wbudowana w płytę główną technologia zarządzania i monitorowania komputera na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6, a także zapewniająca min.: - monitorowanie konfiguracji komponentów komputera, w tym co najmniej:

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
		- CPU, - Pamięć RAM, - HDD, - wersja BIOS, - płyta główna; - zdalna konfiguracja ustawień BIOS, - zdalne przejęcie konsoli tekstowej systemu operacyjnego, - przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM; - zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów) z wbudowanej pamięci nieulotnej,
12	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu).
13	BIOS	BIOS zgodny ze specyfikacją UEFI Możliwość, bez uruchamiania systemu operacyjnego, odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera wraz z datą jego wyprodukowania, ilości i sposobie obłożenia slotów pamięciami RAM, typie procesora wraz z informacją o ilości rdzeni, wielkości pamięci cache L2 i L3, pojemności zainstalowanego dysku twardego, rodzajach napędów optycznych, MAC adresie zintegrowanej karty sieciowej, kontrolerze audio Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS) Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń Możliwość polegająca na kontrolowaniu urządzeń wykorzystujących magistralę komunikacyjną PCI, bez uruchamiania systemu operacyjnego. Pod pojęciem kontroli Zamawiający rozumie funkcjonalność polegającą na blokowaniu/odblokowaniu slotów PCI. Możliwość, bez uruchamiania systemu operacyjnego, ustawienia hasła na poziomie systemu, administratora oraz dysku twardego oraz możliwość ustawienia następującej zależności pomiędzy nimi: brak możliwości zmiany hasła pozwalającego na uruchomienie systemu bez podania hasła administratora. Musi posiadać możliwość ustawienia zależności pomiędzy hasłem administratora a hasłem systemowym tak, aby nie było możliwe wprowadzenie zmian w BIOS wyłącznie po podaniu hasła systemowego. Funkcja ta ma wymuszać podanie hasła administratora przy próbie zmiany ustawień BIOS w sytuacji, gdy zostało podane hasło systemowe. Możliwość włączenia/wyłączenia zintegrowanej karty dźwiękowej, karty sieciowej, portu równoległego, portu szeregowego z poziomu BIOS, bez uruchamiania systemu operacyjnego. Możliwość ustawienia portów USB w trybie „no BOOT", czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. Możliwość wyłączania portów USB w tym: wszystkich portów, tylko portów znajdujących się na przodzie obudowy, tylko tylnich portów. Trwałe oznaczenie w BIOS komputera zawierające nazwę projektu, w ramach którego sprzęt został zakupiony wraz z nazwą i adresem Zamawiającego. Komunikat musi być wyświetlany przy każdym uruchomieniu komputera.
14	Certyfikaty	- Certyfikat ISO9001 lub równoważny dla producenta sprzętu - EnergyStar 5.0 - Deklaracja zgodności CE

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
15	Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji operatora w trybie pracy dysku twardego (WORK) wynosząca maksymalnie 22 dB (**załączyć oświadczenie Wykonawcy**)
16	Warunki gwarancji	-Co najmniej 5 lat -Serwis świadczony na miejscu u klienta -Czas reakcji serwisu - do końca następnego dnia roboczego -Serwis gwarancyjny musi być świadczony przez producenta komputera lub jego autoryzowanego partnera serwisowego lub Wykonawcę
17	Zainstalowane oprogramowanie	Zainstalowany **system operacyjny,** wraz z nośnikiem i przeglądarką internetową w polskiej wersji językowej, niewymagający wpisywania klucza rejestracyjnego lub rejestracji poprzez Internet czy telefon, musi spełniać następujące wymagania: 1. Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek. 2. Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet. 3. Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) 4. Internetowa aktualizacja zapewniona w języku polskim. 5. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 6. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe. 7. Wsparcie dla powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug &Play, Wi-Fi). 8. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer. 9. Interfejs użytkownika działający w trybie graficznym, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta 10. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu 11. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 12. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z co najmniej: poziomu menu, poziomu otwartego okna systemu operacyjnego 13. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. 14. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. 15. Wbudowany system pomocy w języku polskim. 16. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 17. Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji. 18. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. 19. Wsparcie dla logowania przy pomocy smartcard. 20. Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji. 21. System musi posiadać narzędzia służące do administracji, wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
		polityk. 22. Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 lub programów równoważnych, tj. – umożliwiających uruchomienie aplikacji działających we wskazanych środowiskach. 23. Wsparcie dla JScript i VBScript lub równoważnych – możliwość uruchamiania interpretera poleceń. 24. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 25. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową. 26. Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację. 27. Graficzne środowisko instalacji i konfiguracji. 28. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników i pozwalający tworzyć kopie zapasowe. 29. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. 30. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 31. Możliwość przywracania plików systemowych. 32. Możliwość identyfikacji sieci komputerowych, do których jest podłączony komputer, zapamiętywania ustawień i przypisywania do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 33. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). Zainstalowane **oprogramowanie biurowe** musi spełniać następujące wymagania: 1. Wymagania odnośnie interfejsu użytkownika: a) Pełna polska wersja językowa interfejsu użytkownika b) Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych 2. Edytor tekstu winien umożliwiać: a) Edycja i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności b) Wstawianie oraz formatowanie tabel c) Wstawianie obiektów graficznych d) Wstawianie wykresów i tabel z arkusza kalkulacyjnego e) Automatyczne tworzenie spisów treści f) Formatowanie nagłówków i stopek stron g) Określenie układu strony h) Wydruk dokumentów i) Otwarcie, praca i zapis plików w formacie .doc i .docx 3. Arkusz kalkulacyjny winien umożliwiać: a) Tworzenie wykresów liniowych, słupkowych, kołowych b) Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych c) Wyszukiwanie i zamianę danych d) Otwarcie, praca i zapis plików w formacie .xls i .xlsx 4. Program do prezentacji winien umożliwiać: a) Przygotowywanie prezentacji multimedialnych b) Umieszczanie w prezentacjach tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo c) Umieszczanie w prezentacjach tabel i wykresów pochodzących z arkusza kalkulacyjnego d) Otwarcie, praca i zapis plików w formacie .ppt i .pptx

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
		Zainstalowany **program antywirusowy** musi spełniać następujące wymagania: 50. Pełne wsparcie dla oferowanego systemu operacyjnego w wersji 64 bitowej. 51. Interfejsy programu, pomoce i podręczniki w języku polskim. 52. Pomoc techniczna w języku polskim. 53. Multijęzyczny instalator – przynajmniej 5 wersji językowych. 54. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 55. Wykrywanie i usuwanie niebezpiecznych programów: adware, spyware, scareware, phishing, hacktools itp. 56. Wbudowana technologia do ochrony przed rootkitami wykrywająca aktywne i nieaktywne rootkity. 57. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 58. Min. 2 niezależne skanery antywirusowe z 2 niezależnymi bazami sygnatur wirusów wykorzystywane przez skaner dostępowy, skaner na żądanie oraz skaner poczty elektronicznej. 59. Możliwość konfiguracji programu do pracy z jednym (dowolnym) skanerem antywirusowym lub dwoma skanerami antywirusowymi jednocześnie. 60. Technologia kontroli zachowania aplikacji. 61. Kontrola rejestru i pliku autostartu. 62. Kontrola autostartu – możliwość opóźnienia uruchamiania aplikacji z autostartu podczas startu systemu. 63. Skanowanie w trybie bezczynności – pełne skanowanie komputera min. raz na 2 tygodnie uruchamiane i wznawiane automatycznie, podczas gdy nie jest używany. 64. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików na żądanie lub według harmonogramu. 65. 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). 66. Wykrywanie obecności zasilania bateryjnego przed uruchamianiem skanowania. 67. Skanowanie na żądanie pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 68. Możliwość min. 3-stopniowej regulacji obciążenia generowanego przez program 69. Możliwość eksportowania i importowania ustawień programu. 70. Możliwość zabezpieczenia ustawień programu hasłem. 71. Możliwość określania poziomu obciążenia procesora podczas skanowania na żądanie i według harmonogramu. 72. Możliwość wyłączenia komputera po zaplanowanym skanowaniu jeśli żaden użytkownik nie jest zalogowany. 73. Możliwość skanowania dysków sieciowych i dysków przenośnych. 74. Rozpoznawanie i skanowanie wszystkich znanych formatów kompresji. 75. Możliwość definiowania listy plików, folderów i napędów pomijanych przez skaner dostępowy. 76. 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.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
		77. Dedykowany moduł ochrony bankowości internetowej, nie bazujący na bazach sygnatur wirusów jak i analizie heurystycznej (heurystyce). Moduł ten ma współpracować z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 78. Skanowanie i oczyszczanie poczty przychodzącej POP3 w czasie rzeczywistym, zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 79. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. 80. Możliwość definiowania różnych portów dla POP3, SMTP i IMAP na których ma odbywać się skanowanie. 81. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. 82. Skanowanie ruchu HTTP. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. 83. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 84. Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie. 85. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. 86. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń powinny być w pełni anonimowe. 87. Aktualizacja dostępna z bezpośrednio Internetu, lub offline – z pliku pobranego zewnętrznie. 88. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. 89. Możliwość określenia częstotliwości aktualizacji w odstępach min. 1 godzinowych. 90. Program wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, antyspam, skaner HTTP). 91. Raportowanie wykrytych zagrożeń i wszystkich przeprowadzonych działań. 92. Kreator płyt startowych umożliwiających nagrywanie płyt skanujących komputer bez udziału systemu operacyjnego. 93. Kreator musi nagrywać obraz płyty bezpośrednio na nośnik CD lub zapisać go na dysku. 94. System operacyjny wykorzystywany przez płytę startową musi umożliwiać uaktualnienie sygnatur wirusów przez Internet przed rozpoczęciem skanowania. 95. System operacyjny wykorzystywany przez płytę startową musi automatycznie wykrywać sieci bezprzewodowe. 96. Interfejs programu musi informować o terminie ważności licencji. 97. Program musi wyświetlać monity o zbliżającym się zakończeniu licencji, a także powiadamiać o zakończeniu licencji. 98. Użytkownik musi mieć możliwość podejrzenia numeru rejestracyjnego zastosowanego w programie. 99. Prawo do bezpłatnej aktualizacji baz wirusów i innych zagrożeń przez okres 3 lat od dnia odbioru przez Zamawiającego
18.	Wymagania dodatkowe	Porty wbudowane w płytę główną: RS232, VGA, 2 x PS/2, 2 x DisplayPort , min. 10 portów USB wyprowadzonych na zewnątrz komputera: 4x USB 3.0 (min. 2 z przodu obudowy), 6x USB 2.0; wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. porty słuchawek i mikrofonu na przednim oraz

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
		tylnym panelu obudowy. Karta sieciowa 10/100/1000 Ethernet RJ 45, wspierająca obsługę WoL, PXE 2.1, umożliwiająca zdalny dostęp do wbudowanej sprzętowej technologii zarządzania komputerem z poziomu konsoli zarządzania - niezależnie od stanu zasilania komputera - łącznie z obsługą stanu S3 (uśpienie) oraz S4-S5 (hibernacja i wyłączenie); Płyta główna wyposażona w : min. 2 złącza PCI Express x16 w tym jedno elektryczne jak PCIe x4, min. 4 złącza DIMM z obsługą do 16GB pamięci RAM, min. 3 złącza SATA w tym 2 szt. SATA 3.0; Klawiatura USB w układzie polski programisty Mysz optyczna USB z dwoma klawiszami oraz rolką (scroll) Nagrywarka DVD +/-RW Dołączony nośnik ze sterownikami

Monitor do zestawów pkt 5.6.1 ……..200 szt.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne monitora
1	Przekątna ekranu	min. 19”
2	Powłoka powierzchni ekranu	Antyodblaskowa
3	Typ podświetlenia	LED
4	Rozmiar plamki	Maks. 0,27 mm
5	Jasność	250 cd/m2
6	Kontrast	min. 1000:1
7	Kąty widzenia (pion/poziom)	160/170 stopni
8	Czas reakcji matrycy	max 5ms (od czerni do bieli)
9	Rozdzielczość nominalna	1600 x 900 przy 60Hz
10	Format obrazu	16:9
11	Częstotliwość odświeżania poziomego	30 – 80 kHz
12	Częstotliwość odświeżania pionowego	60 – 70 Hz
13	Pochylenie monitora	W zakresie od 5 do przodu i 20 stopni wstecz
14	Złącze	15-stykowe złącze D-Sub, złącze DisplayPort lub DVI-D lub HDMI,
15	Pobór energii typowy	Max 15W
16	Głośniki	Wbudowane lub zintegrowane z monitorem o mocy min. 10W
17	Gwarancja	-Co najmniej 5 lat -Serwis świadczony na miejscu u klienta -Czas reakcji serwisu - do końca następnego dnia roboczego -Serwis gwarancyjny musi być świadczony przez producenta komputera, jego autoryzowanego partnera serwisowego lub Wykonawcę
18	Certyfikaty	TCO 6.0, Energy Star 5.0

5.7 Usługi wsparcia technicznego i serwisu gwarancyjnego systemu. (sprzętu komputerowego oraz sieci szerokopasmowej)

5.7.1 Wsparcie techniczne i obsługa serwisowa zestawów komputerowych i oprogramowania .

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

Minimalne warunki świadczenia usług :

- 5-letnia gwarancja liczona od dnia podpisania protokołu odbioru końcowego zestawów komputerowych, świadczona na miejscu u BO potwierdzona kartą gwarancyjną.
- przyjmowanie i obsługa zgłoszeń gwarancyjnych w godz. 08.00 – 18.00, w dni robocze poprzez wydzielony telefon serwisowy, fax ,e-mail
- czas reakcji serwisu - do końca następnego dnia roboczego
- świadczenia usług wsparcia technicznego oraz serwisu w zakresie sprzętu i oprogramowania dostarczonego w ramach zamówienie w okresie realizacji umowy z Zamawiającym poprzez wydzielony telefon serwisowy, fax ,e-mail
- usunięcie usterki w ciągu najpóźniej 3 dni roboczych od momentu zgłoszenia. Przez usterkę rozumie się wadę techniczną, która nie uniemożliwia całkowicie korzystania z komputera, a jedynie powoduje pogorszenie jakości jego działania;
- usunięcie awarii w ciągu najpóźniej 2 dni roboczych od momentu zgłoszenia. Przez awarie rozumie się całkowitą niemożność użytkowania komputera;
- 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

Inne wymagania wobec Wykonawcy :

- Gwarant udostępnia Zamawiającemu BIOS, firmware i sterowniki na płytach CD. Dodatkowo Zamawiający i Beneficjenci ostateczni będą mieli dostęp do aktualnych sterowników poprzez wskazaną przez Wykonawcę stronę internetową.
- Gwarant ponosi koszty napraw gwarancyjnych (serwisowych), włączając w to koszt części. W przypadku, gdy naprawy nie uda się zrealizować w siedzibie BO , Gwarant ponosi również koszty transportu.
- Prowadzenie bazy napraw z możliwością dostępu on-line przedstawiciela Zamawiającego.

5.7.2. Serwis gwarancyjny i utrzymanie infrastruktury sieci szerokopasmowej

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

Minimalne warunki świadczenia oraz zakres usług :

a)3-letnia gwarancja liczona od dnia podpisania protokołu odbioru końcowego sieci szerokopasmowej , świadczona w miejscu instalacji .

b)bieżące monitorowanie infrastruktury i wykrywanie awarii oraz ich usuwanie w ciągu maksymalnie 24 godzin w okresie realizacji umowy z Zamawiającym.
W przypadku braku możliwości naprawy lub usunięcia awarii w ciągu 24 godzin, zapewnienie urządzeń zastępczych na czas naprawy w celu zachowania ciągłości pracy sieci;

c) obsługa procedur gwarancyjnych w przypadku kiedy uszkodzenia i awarie dotyczą urządzeń sieciowych objętych gwarancją.

d) aktualizacja oprogramowania urządzeń transmisyjnych ,sieciowych, w tym aktualizacja firmware'ów, oraz wykonywanie update'ów systemu bezpieczeństwa – zgodnie z zaleceniami producentów urządzeń w okresie realizacji umowy z Zamawiającym

e) okresowa konserwacja oraz przegląd elementów infrastruktury teleinformatycznej w okresie gwarancji.

VI. OGÓLNE WARUNKI WYKONANIA I ODBIORU ROBÓT

1. Pozostałe wymagania od Wykonawców

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

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

2. Szkolenia dla administratorów sieci

W ramach robót wymagane jest aby Wykonawca sieci przeprowadził szkolenia dla wyznaczonych pracowników Operatora Infrastruktury (podmiot ten zostanie wyłoniony w odrębnym postępowaniu przetargowym) w zakresie:

- Konfiguracji i zarządzania radioliniami
- Podstawowej konfiguracji i zarządzania urządzeniami aktywnymi sieci
- Administracja i zarządzanie bezprzewodowa siecią dostępową LTE / WiFi
- Zarządzania systemem LMS
- Polityki autentykacji i autoryzacji użytkowników sieci
- Wykonywania kopii bezpieczeństwa, plików konfiguracyjnych itp.

3. Dokumenty odbioru końcowego

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

VII. CZĘŚĆ INFORMACYJNA PROGRAMU

7.1 Akty prawne i rozporządzenia:

1.1 Ustawa o wspieraniu rozwoju usług i sieci telekomunikacyjnych Dz. U. nr 106 z dnia 16 czerwca 2010 r. , poz. 675
1.2 „Ustawa Prawo telekomunikacyjne z dnia 16 lipca 2004 roku".
1.3 „Ustawa o świadczeniu usług droga elektroniczna 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.

7.2 Ramy prawne Komisji Europejskiej w sektorze komunikacji elektronicznej

1.1 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.);
1.2 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.);
1.3 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.);
1.4 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.) ;
1.5 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.);

1.6 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.);
1.7 Rozporządzenie (EC) 2887/2000 o niezależnym dostępie do pętli lokalnych

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

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

Załącznik 1 rozmieszczenie Beneficjentów ostatecznych

lp	ADRES ZAMELDOWANIA
1	WOŁOMIN, POLNA 11 M. 2
2	LEŚNIAKOWIZNA, UL. KASPRZYKIEWICZA 151
3	CZARNA, UL. WITOSA 43
4	WOŁOMIN, KOLEJOWA 1 M. 1
5	DUCZKI, RĘCZAJSKA 16
6	WOŁOMIN, SŁONECZNA BL. 8 M. 3
7	WOŁOMIN, CHROBREGO 1 M. 140
8	DUCZKI, NOWA 15
9	WOŁOMIN, WARSZAWSKA 32 M. 4
10	WOŁOMIN, ARMII KRAJOWEJ 64 BL. 10 M. 18
11	WOŁOMIN, SIKORSKIEGO 15 M. 8
12	WOŁOMIN, SIKORSKIEGO 15 M. 1
13	WOŁOMIN, KOŚCIELNA 68 M. 1
14	WOŁOMIN, NAUKOWSKIEGO 28
15	WOŁOMIN, AL. ARMII KRAJOWEJ 64 BL. 10 M. 14
16	OSSÓW, ROZWADOWSKIEGO 93, 05-230 KOBYŁKA
17	WOŁOMIN, BŁOŃSKA 53
18	WOŁOMIN, LEGIONÓW 57
19	LIPINKI, WIOSENNA 9
20	WOŁOMIN, MICKIEWICZA 49B
21	WOŁOMIN, AL. NIEPODLEGŁOŚCI 9
22	WOŁOMIN, PIŁSUDSKIEGO 7/11 M. 34
23	WOŁOMIN, WILEŃSKA 61 M. 4
24	WOŁOMIN, KOŚCIELNA 12 M. 18/19
25	WOŁOMIN, WILEŃSKA 78 M. 17
26	WOŁOMIN, WILEŃSKA 45 M. 7
27	WOŁOMIN, ANDERSA 28
28	ZAGOŚCINIEC, MOKRA 2
29	DUCZKI, SZOSA JADOWSKA 21B
30	WOŁOMIN, KRÓLOWEJ JADWIGI 7/14
31	WOŁOMIN, SIENKIEWICZA 12 M. 5
32	WOŁOMIN, AL. ARMII KRAJOWEJ 64 11/13
33	LIPINKI, KLONOWA 26
34	WOŁOMIN, BŁOTNA 15
35	WOŁOMIN, WILEŃSKA 4 M. 6
36	NOWE LIPINY, DUCZKOWSKA 26
37	WOŁOMIN, MONIUSZKI 1 M. 14
38	WOŁOMIN, CHROBREGO 3 M. 46
39	WOŁOMIN, OGRODOWA 2 M. 2
40	WOŁOMIN, OGRODOWA 2
41	MAJDAN, UL. RACŁAWICKA 39
42	WOŁOMIN, KILIŃSKIEGO 2
43	WOŁOMIN, DWORSKA 9

44	WOŁOMIN, WARSZAWSKA 11 M. 10
45	DUCZKI, ZACHODNIA 12
46	WOŁOMIN, WIERZBOWA 3
47	WOŁOMIN, SIENKIEWICZA 32 M. 9
48	WOŁOMIN, SŁONECZNA 11 M. 6
49	WOŁOMIN, POLSKA 34/4
50	WOŁOMIN, PRĄDZYŃSKIEGO 20A M. 56
51	WOŁOMIN, SIKORSKIEGO 117
52	DUCZKI, RĘCZAJSKA 10
53	WOŁOMIN, WILEŃSKA 48 M. 12
54	WOŁOMIN, SIKORSKIEGO 44
55	WOŁOMIN, POLSKA 31
56	WOŁOMIN, LEGIONÓW 109
57	STARE LIPINY, PORANEK 13
58	WOŁOMIN, SIKORSKIEGO 46
59	WOŁOMIN, KOŚCIELNA 22 M. 11
60	WOŁOMIN, BŁOTNA 23/22
61	WOŁOMIN, BRZOZOWA 12 M. 12
62	WOŁOMIN, LIPIŃSKA 2 M. 54
63	WOŁOMIN, SIKORSKIEGO 75
64	NOWE LIPINY, ROLNA 20
65	WOŁOMIN, WARSZAWSKA 11 M. 6
66	LEŚNIAKOWIZNA, UL. KASPRZYKIEWICZA 216
67	WOŁOMIN, WARSZAWSKA 7 M. 1
68	NOWE LIPINY, ROLNA 53
69	WOŁOMIN, MONIUSZKI 7 M. 14
70	LEŚNIAKOWIZNA, UL. KASPRZYKIEWICZA 99
71	WOŁOMIN, MONIUSZKI 29
72	WOŁOMIN, KRESOWA 43
73	LIPINKI, KLONOWA 5A
74	WOŁOMIN, SIKORSKIEGO 88 M. 32
75	WOŁOMIN, ŚREDNIA 1 M. 2
76	WOŁOMIN, LIPIŃSKA 32A M. 29
77	MAJDAN, RACŁAWICKA 73
78	WOŁOMIN, WARSZAWSKA 28/15
79	CZARNA, WITOSA 105
80	CZARNA, CZARNIECKIEGO 42
81	WOŁOMIN, AL. ARMII KRAJOWEJ 64 BL. 1 M. 4
82	CZARNA, WITOSA 19
83	WOŁOMIN, LEŚNA 9
84	WOŁOMIN, MATEJKI 5
85	WOŁOMIN, 1 MAJA 3 M. 38
86	WOŁOMIN, POLNA 19
87	WOŁOMIN, AL NIEPODLEGŁOŚCI 10 M. 31
88	WOŁOMIN, SIENKIEWICZA 18/5
89	ZAGOŚCINIEC, JOŁOWCOWA 22
90	WOŁOMIN, MICKIEWICZA 4
91	WOŁOMIN, WARSZAWSKA 31 M. 2
92	WOŁOMIN, OS. SŁONECZNA BL. 12 M. 23
93	WOŁOMIN, SŁAWKOWSKA 26
94	WOŁOMIN, FIELDORFFA 16 M. 6
95	WOŁOMIN, LESZCZYŃSKA 21
96	WOŁOMIN, KAZIMIERZA WLK. 4 M/5
97	ZAGOŚCINIEC, SZKOLNA 30
98	NOWE LIPINY, BŁĘKITNA 4

99	WOŁOMIN, ARMII KRAJOWEJ 15A
100	CZARNA, CHABROWA 1A
101	WOŁOMIN, SŁONECZNA 3
102	WOŁOMIN, GEODETÓW 14
103	WOŁOMIN, PRUSA 7
104	WOŁOMIN, DUCZKOWSKA 54
105	WOŁOMIN, 6 WRZEŚNIA 2 M. 4
106	STARE GRABIE, GŁÓWNA 62
107	WOŁOMIN, WILEŃSKA 8 M. 8
108	WOŁOMIN, ZŁOTA 46
109	WOŁOMIN, KURKOWA 46
110	WOŁOMIN, ORGIDA 5 M. 2
111	WOŁOMIN, KAZIMIERZA WLK. 8 M. 17
112	WOŁOMIN, 6 WRZEŚNIA 3 M. 10
113	ZAGOŚCINIEC, NADRZECZNA 6
114	WOŁOMIN, LESZCZYŃSKA 9
115	WOŁOMIN, PIŁSUDSKIEGO 23
116	WOŁOMIN, 1 MAJA 90C
117	LIPINKI, WIOSENNA 7
118	LIPINKI, PIASKOWA 3A
119	WOŁOMIN, WARSZAWSKA 24/3
120	WOŁOMIN, WARSZAWSKA 13 M. 13
121	WOŁOMIN, KOŚCIELNA 45/1
122	WOŁOMIN, POLNA 9 M. 4
123	WOŁOMIN, ZIELONA 59 M. 1
124	WOŁOMIN, KOŚCIUSZKI 15 M. 2
125	LIPINKI, SŁONECZNA 28
126	WOŁOMIN, GŁOWACKIEGO 52
127	WOŁOMIN, TĘCZOWA 20A
128	TURÓW, HALLERA 81, 05-230 KOBYŁKA
129	WOŁOMIN, LESZCZYŃSKA 10
130	WOŁOMIN, NIEPODLEGŁOŚCI 12 M 66
131	NOWE LIPINY, KRZYŻOWA 31
132	CZARNA, RADZYMIŃSKA 14
133	ZAGOŚCINIEC, STULECIA 123
134	WOŁOMIN, KOŚCIELNA 66/13
135	OSSÓW, MATAREWICZA 65, 05-230 KOBYŁKA
136	WOŁOMIN, SIKORSKIEGO 1A/10
137	WOŁOMIN, SIENKIEWICZA 12 M. 6
138	MAJDAN, RACŁAWICKA 83
139	WOŁOMIN, WILEŃSKA 74 M. 9
140	WOŁOMIN, KLONOWA 6A
141	WOŁOMIN, WILEŃSKA 5 M. 1
142	WOŁOMIN, SUWALSKA 11A
143	LIPINKI, KLONOWA 2
144	WOŁOMIN, KOBYŁKOWSKA 28 M. 17
145	WOŁOMIN, LIPIŃSKA 50/1
146	OSSÓW, ROZWADOWSKIEGO 12
147	WOŁOMIN, MICKIEWICZA 2/7
148	WOŁOMIN, MIŁA 38
149	DUCZKI, POPRZECZNA 13
150	NOWE GRABIE 59
151	NOWE GRABIE 60
152	WOŁOMIN, AKACJOWA 11
153	STARE GRABIE, DWORCOWA 15

154	WOŁOMIN, WARSZAWSKA 1 M.4
155	WOŁOMIN, SIKORSKIEGO 88/35
156	WOŁOMIN, KOŚCIELNA 41/3
157	WOŁOMIN, POLNA 2 M.13
158	ZAGOŚCINIEC, STULECIA 184
159	WOŁOMIN, OKOPOWA 6A
160	NOWE LIPINY, BATALIONÓW CHŁOPSKICH 56
161	DUCZKI, MAJDAŃSKA 4
162	WOŁOMIN, WILEŃSKA 66 M.18
163	WOŁOMIN, WILEŃSKA 45/15
164	LIPINKI, WIOSENNA 16
165	WOŁOMIN, SŁOWACKIEGO 38
166	WOŁOMIN, WILEŃSKA 4 M.4
167	WOŁOMIN, FIELDORFA 14 M.4
168	WOŁOMIN, KOŚCIELNA 12 M.5
169	WOŁOMIN, PARKOWA 6
170	WOŁOMIN, WILEŃSKA 25/1
171	ZAGOŚCINIEC, KOLEJOWA 9A
172	WOŁOMIN, ŚREDNIA 29A
173	WOŁOMIN, KOŚCIELNA 62 M.8
174	WOŁOMIN, WILEŃSKA 3 M.8
175	CZARNA, WITOSA 49
176	ZAGOŚCINIEC, MOKRA 7
177	WOŁOMIN, WARSZAWSKA 10 M.10
178	WOŁOMIN, WILEŃSKA 4 M.3
179	WOŁOMIN, MONIUSZKI 7 M.7
180	WOŁOMIN, LIPIŃSKA 2 M.69
181	ZAGOŚCINIEC, 100-LECIA 80B
182	LIPINKI, KWIATOWA 16
183	WOŁOMIN, PRZYJACIELSKA 10
184	WOŁOMIN, ŻELAZNA 12 M.7
185	WOŁOMIN, FIELDORFA 2 M.5
186	WOŁOMIN, CHROBREGO 1 M.110
187	WOŁOMIN, MIESZKA 1 14B M.24
188	WOŁOMIN, KOŚCIELNA 31 M.10
189	STARE LIPINY, KWITNĄCA 9
190	WOŁOMIN, ORZECHOWA 5
191	WOŁOMIN, AL. NIEPODLEGŁOŚCI 187
192	WOŁOMIN, POLSKA 2
193	WOŁOMIN, PIŁSUDSKIEGO 7/11 M.12
194	DUCZKI, TURYSTYCZNA 4
195	WOŁOMIN, SIKORSKIEGO 24 M.17
196	WOŁOMIN, WIEJSKA 5/7
197	WOŁOMIN, ŻWIRKI I WIGURY 6
198	ZAGOŚCINIEC, 100-LECIA 44
199	MAJDAN, RACŁAWICKA 103
200	WOŁOMIN, OS. SŁONECZNA BL. 13 M. 13