Załącznik nr 6 do SIWZ

Znak: OS.0303/5/09

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

(Program funkcjonalno – użytkowy)

Budowa sieci bezprzewodowej, usługa dostępu do Internetu, dostawa sprzętu komputerowego, serwis sieci i sprzętu w ramach projektu: „Przeciwdziałanie wykluczeniu cyfrowemu – Internet dla mieszkańców Gminy Dobre”

Etapy realizacji zamówienia:

- Wykonanie projektu sieci radiowej – do 28.02.2010 r.
- Budowa stacji bazowych – do 31.05.2010 r.
- Wyposażenie serwerowni – do 31.05.2010 r.
- Budowa stacji przekaźnikowych – do 30.06.2010 r.
- Montaż urządzeń odbiorczych WiFi – do 30.06.2010 r.
- Dostawa komputerów wraz z oprogramowaniem – do 30.06.2010 r.
- Serwis sieci i urządzeń – od 01.03.2010 r. do 31.12.2012 r.
- Usługa dostępu do Internetu - od 01.03.2010 r. do 31.12.2012 r.

1. Wykonanie projektu sieci radiowej

Zamawiający wymaga wykonania całości dokumentacji projektowej związanej z budowaną siecią radiową oraz przygotowania całości dokumentacji niezbędnej do uzyskania pozwoleń radiowych na używanie radiowych urządzeń nadawczo – odbiorczych pracujących w ramach Sieci, pozwoleń budowlanych, zgłoszeń robót budowlanych.

Zamawiający wymaga wykonania projektu sieci radiowej w technologii WiMAX lub LMDS zapewniającej podłączenie do Internetu stu dwudziestu beneficjentów końcowych za pomocą:

1.1. co najmniej jednego masztu umożliwiającego instalację projektowanej stacji bazowej, przystosowanego do przenoszenia naporów wiatru do 5 m^2 powierzchni antenowej zlokalizowanego na istniejącym budynku lub na gruncie stanowiących własność zamawiającego lub wskazanym przez zamawiającego po uprzednim ustaleniu.
1.2. co najmniej 1 stacji bazowej pracujących w standardzie WIMAX / LMDS o minimalnych parametrach określonych w pkt. 2.1 lub 2.2,
1.3. W przypadku projektowania więcej niż 1 stacji bazowej konieczne jest zaprojektowanie i uwzględnienie linii radiowej zgodnie z pkt. 2.3,
1.4. co najmniej 26 stacji przekaźnikowych WIMAX / LMDS - WIFI o minimalnych parametrach określonych w pkt. 3,
1.5. 120 urządzeń odbiorczych pracujących w standardzie 802.11a / 802.16d zamontowanych na budynkach beneficjentów końcowych o minimalnych parametrach określonych w pkt. 4.

Wykonawca zobowiązany jest do wybrania optymalnej lokalizacji stacji bazowych zapewniającej zasilenie wszystkich stacji przekaźnikowych.
Transmisja pomiędzy głównym węzłem a stacjami bazowymi realizowana będzie przy wykorzystaniu linii radiowych pracujących w paśmie licencjonowanym, o parametrach określonych w punkcie 2.3.

Wykonawca zobowiązany jest do wybrania optymalnej lokalizacji instalacji stacji przekaźnikowych zapewniających pokrycie co najmniej 90% powierzchni gminy Dobre i obejmujących zasięgiem co najmniej 95% ludności gminy Dobre

Wymagania odnośnie projektu:

Zamawiający udostępni listę beneficjentów końcowych projektu (lokalizacje) po podpisaniu umowy.

W projekcie sieci radiowej Wykonawca zobowiązany jest do:

1. Zaplanowania lokalizacji instalacji stacji bazowych, ustalenie lokalizacji (wysokość zainstalowania) i projektu z właścicielem masztu / terenu, uzyskanie wszystkich niezbędnych pozwoleń, w razie potrzeby ustalenie i skoordynowanie projektu z innymi najemcami, przygotowanie listy urządzeń (zawierających symbol producenta oraz inne niezbędne elementy identyfikacyjne), anten zamontowanych na maszcie (zawierających specyfikacje anten i azymuty wiązki głównej anteny, wysokość instalacji, kąty pochylenia), długość fiderów (kabli) łączących element zewnętrzny z urządzeniami zamontowanymi w szafie, rodzaje użytych wtyków.
2. Przygotowanie projektu technicznego i budowlanego masztu zgodnie z obowiązującymi normami i przepisami,
3. Zaplanowanie lokalizacji stacji przekaźnikowych WiMAX/LMDS - WIFI, opisania miejsca instalacji podając adres oraz współrzędne geograficzne, typ obiektu, wysokość planowanego masztu, wysokości budynku (jeżeli urządzenia zaplanowane są do instalacji na budynku),

załączenia zdjęcia budynku. Przygotować wszystkie niezbędne dokumenty do uzyskania odpowiednich pozwoleń wymaganych przepisami prawa budowlanego.

4. Przedstawienia wyniku symulacji komputerowej ilustrującej szkielet wszystkich zaplanowanych połączeń w sieci (stacji bazowych + radiolinii + stacji przekaźnikowych).
5. Przedstawienia wyniku symulacji komputerowej ilustrującej prognozowany zasięg sieci wraz z poziomami sygnału.
6. Przedstawienia wyniku symulacji komputerowej ilustrującej prognozowany zasięg każdej stacji przekaźnikowej wraz z poziomami sygnału.

Warunkiem koniecznym do przystąpienia do budowy infrastruktury jest akceptacja projektu radiowego przez Zamawiającego, uzyskanie niezbędnych pozwoleń radiowych, uzyskanie aprobaty właścicieli obiektów (masztów, gruntów, kominów) wraz z ustaleniami z pozostałymi najemcami znajdującymi się na danym obiekcie.
Koszty związane z wykonaniem projektu należy wliczyć w koszty budowy infrastruktury (stacji bazowych i przekaźnikowych).

2. Stacje bazowe (min. 1 szt.)

Zamawiający wymaga zainstalowania stacji bazowych i radiolinii zgodnie z projektem sieci. Wykonawca zobowiązany jest do przygotowania dokumentacji niezbędnej do uzyskania pozwoleń na budowę lub zgłoszeń robót budowlanych.
Po ukończeniu budowy stacji bazowych Wykonawca zobowiązany jest do wykonania dokumentacji powykonawczej zgodnej z projektem sieci i wykonania zdjęcia każdej zainstalowanej stacji bazowej.

a) Oferowany system radiowy WIMAX musi spełniać nw. wymagania minimalne:

- szerokopasmowy system radiowy klasy WiMAX
- praca w paśmie licencjonowanym w zakresie 3.4GHz – 3.6GHz lub 3.6GHz-3.8GHz
- praca stacji bazowej w trybie full-duplex w dziedzinie częstotliwości (FDD) z odstępem kanałów dupleksowych wynoszącym 100MHz
- możliwość wykorzystania kanałów radiowych zorganizowanych na bazie planów podziału pasma 3.5A7; 3.5A3.5 i 3.5A1.75 lub 3.7A7; 3.7A3.5 i 3.7A1.75
- stacja bazowa musi posiadać możliwość pracy w kanale 1,75MHz, 3,5 MHz i 7 MHz (jednocześnie ustawiana tylko jedna z tych szerokości kanałów)
- zasięg maksymalny nie mniej niż 15 km
- interfejs stacji bazowej 100/1000BaseT
- interfejsy sieciowe w jednostkach abonenckich: 10/100BaseT
- maksymalna wydajność (netto na protokole TCP/IP) mogąca być dostarczona do jednostki abonenckiej nie mniej niż 10 Mbps
- ilość jednostek abonenckich nie mniejsza niż 256 na stacje bazową
- co najmniej 4 klasy priorytetów dla usług sieciowych
- zapewnienie jakości transmisji (QoS) dla każdej z usług sieciowych poprzez osobno konfigurowalne parametry
- zarządzanie siecią z centralnego punktu poprzez protokół SNMP
- maksymalna moc promieniowania EIRP nie więcej niż 15 Watt
- możliwość zastosowania anten z polaryzacją liniową H i V
- możliwość zapewnienia kilku (minimum 5) różnych odseparowanych od siebie strumieni danych z możliwością przydzielenia różnej przepustowości każdemu strumieniowi i różnej klasy QoS w obrębie jednego terminala abonenckiego – z zastosowaniem tagowania VLAN 802.1q
- możliwość dynamicznego zarządzania pasmem (w przypadku gdy dany abonent nie korzysta z pasma - pasmo musi być dostępne dla innych klientów systemu)

- wydajność sieciowa systemu w warstwie drugiej (L2) nie mniejsza niż 70% wydajności radiowej
- wydajność radiowa systemu nie mniej niż 3.4 bita/Hz
- dynamiczna obsługa modulacji BPSK, QPSK, 16QAM, 64QAM
- możliwość zastosowania różnej modulacji dla ruchu od abonenta do stacji bazowej (uplink) i ruchu od stacji bazowej do abonenta (downlink) dla dowolnego terminala abonenckiego
- możliwość zastosowania różnej modulacji dla różnych terminali abonenckich podłączonych do jednego sektora stacji bazowej
- możliwość budowy stacji bazowej o pokryciu 360 stopni przy pomocy czterech sektorów każdy o pokryciu 90 stopni
- system musi posiadać możliwość pracy w warunkach braku widoczności radiowej zrealizowanej w oparciu o modulację OFDM 256 FFT
- system musi być zgodny ze specyfikacją IEEE 802.16
- system powinien posiadać certyfikat WiMAX Forum (jeśli WiMAX Forum określiło profil systemu w danym paśmie);
- system musi wspierać usługi głosowe VoIP w oparciu o protokół SIP
- system radiowy musi być dostępny komercyjnie w chwili składania oferty
- możliwość poprawy jakości linku radiowego za pomocą rozwiązań typu „antenna diversity" 2-go rzędu
- system musi umożliwiać poprawę jakości połączeń głosowych za pomocą zintegrowanych lub zewnętrznych mechanizmów/aplikacji
- system musi umożliwiać obsługę protokołu DHCP z opcją 82
- system musi posiadać mechanizmy zapobiegające obniżeniu pojemności sektora przez terminale pracujące ze zbyt niską modulacją
- system musi posiadać wbudowane narzędzia analizujące zajętość pasma radiowego przez inne systemy

b) Oferowany system radiowy LMDS musi spełniać nw. wymagania minimalne:

- praca w licencjonowanym paśmie pracy 26 lub 28 Ghz
- pracujący w technologii FDD TDMA.
- dostarcza usługi, E1, FE1, LL, IP z maksymalną szybkością transmisji do abonenta 34Mb/s
- budowa modularna części wewnętrznej stacji bazowej (IDU – indoor unit), zamkniętej w kompaktowej obudowie o identycznej wielkości i wyglądzie jak terminale abonenckie w celu ogranicza krytycznego elementu systemu mogące ulec uszkodzeniu.
- Jednostka radiowa RFU musi być zintegrowana z anteną co umożliwia montaż na zewnątrz,
- pojedyncza jednostka RFU obsługuje jeden sektor stacji bazowej w trybie multi-carrier.
- możliwość czterokrotnego (4 x 34MB/s) zwiększenia pojemności pojedynczego sektora stacji bazowej systemu przy pomocy multipleksera bez potrzeby rozbudowy zewnętrznej części radiowej
- możliwość pracy z obydwiema polaryzacjami: pionową (V) i poziomą (H)
- użyteczna efektywność spektralna > 2 bit/s/Hz
- możliwość zastosowania anten 90 i 180 stopniowych
- praca w różnych planach podziału pasma, tzn. z szerokościami kanałów użytkowych 7MHz (plan 26A7), 14MHz (plan 26A14) i 28MHz (plan 26A28) podobnie dla pasma 28 GHz
- przepływność pojedynczego sektora stacji bazowej bazującego na kanale 28MHz powyżej 65Mbps
- budżet łącza radiowego systemu zapewniający zasięg użyteczny do 5km w warunkach strefy klimatycznej H
- zapewnienie interfejsów 10/100Base-T oraz E1 (G.703 lub G.704), zarówno po stronie stacyjnej, jak i abonenckiej

- zapewnienie przeźroczystości systemu w warstwie 2 transmisji typu Ethernet
- możliwość zastosowania pełnej redundancji sprzętowej stacji bazowej, tzn. części zewnątrzbudynkowej, części wewnątrzbudynkowej i interfejsów stacyjnych
- możliwość groomingu usług FE1, tzn. grupowania usług typu Nx64k z wielu terminali w pojedynczym porcie E1 stacji bazowej
- terminale abonenckie systemu muszą zapewniać przepływność do 34Mbps
- możliwość priorytyzacji ruchu IP bazujące na DSCP
- możliwość separacji ruchu IP wielu abonentów dołączonych do jednego terminala z użyciem VLAN bazujących na standardzie 802.1q

Koszty budowy stacji bazowych muszą uwzględniać również koszty dostawy i uruchomienia radiolinii oraz systemu zarządzania siecią, szaf, siłowni, masztów oraz wszystkich elementów niezbędnych do uruchomienia i prawidłowego działania infrastruktury.

2.1. Wymagania minimalne dla stacji bazowej systemu WiMAX

- interfejs stacji bazowej 100/1000BaseT
- możliwość zastosowania anten z polaryzacją liniową H i V
- możliwość budowy stacji bazowej o pokryciu 360 stopni przy pomocy czterech sektorów każdy o pokryciu 90 stopni
- stacja bazowa powinna posiadać certyfikat WiMAX Forum (jeśli WiMAX Forum określiło profil systemu w danym paśmie)
- możliwość poprawy jakości linku radiowego za pomocą rozwiązań typu „antenna diversity" 2-go rzędu
- możliwość zastosowania wersji z wymiennymi kartami, jak również wersji zintegrowanej w obudowie typu kompaktowego (tzw. „pizza box")
- możliwość wymiany wersji kompaktowej na wersję z wymiennymi kartami (lub vice versa) bez konieczności wymiany urządzeń zewnętrznych stacji bazowej
- sektor stacji bazowej musi posiadać możliwość pracy w kanale 1,75MHz, 3,5 MHz i 7 MHz (jednocześnie ustawiana tylko jedna z tych szerokości kanałów)
- wbudowany miernik jakości transmisji danych BER.

2.2. Wymagania minimalne dla stacji bazowej systemu LMDS

- Montaż w racku 19" lub 21"
- wyposażenie w urządzenie nadawczo-odbiorcze do transmisji radiowej
- stacja z możliwością wyposażenia w 4 sektory
- zastosowane anteny 90 stopniowe
- możliwość umieszczenia nadajnika radiowego w odległości co najmniej 100 m od stacji bazowej
- Interfejsy E1 (min. 32)
- Interfejsy Ethernet 10/100 (min.2)
- Lokalny port konsoli
- budowa modularna pozwalająca na rozbudowę stacji bazowej
- Możliwość budowy konfiguracji redundantnej części zewnętrznej i jednostek podstawowych stacji bazowej
- dedykowany port zarządzania
- możliwość zarządzania po wydzielonym VLAN przez port transmisji danych
- zasilanie 48 VDC
- funkcja analizy widma
- funkcja testowania BER
- dedykowany system zarządzania

2.3 Wymagania minimalne dla radiolinii

Pojemność użytkowa radiolinii

System powinien umożliwiać transmisję sygnału głównego o pojemności 50 Mb/s, 100Mb/s, 150 Mb/s, 200 oraz 300 Mb/s full duplex. Zmiana przepływności powinna odbywać się poprzez programową rekonfigurację IDU (bez konieczności wymiany tego modułu przy każdorazowej zmianie przepływności).

Urządzenie powinno posiadać porty do przesyłania danych: 2xGigabitEthernet 10/100/1000BASE-T z możliwością zwiększenia ilości portów GigabitEtherent na medium miedziane i optyczne. Urządzenie powinno zawierać minimum 4 porty E1 G703 z możliwością rozszerzenia do 32 portów E1 i do zarządzania: port USB oraz jeden port 10Base-T.

Wymaga się, aby strumienie Ethernetowy pracowały w technologii nativeEthernet bez mapowania na inną technologię (PDH, SDH). Wymaga się, aby strumienie 2Mb/s dostępne w interfejsie radiowym a niewykorzystane przez port Ethernet posiadały możliwość dołączenia do portów 2Mb/s G.703 na panelu czołowym urządzenia. Wymagane jest, aby urządzenie posiadało do 4 portów E1 G703 dostępnych z panel czołowego.

Wymaga się, aby urządzenie oferowało pełną dowolność w przypisywaniu zasobów radiowych do portów Ethernet i TDM.

Kanały utrzymaniowe

Oczekuje się, że urządzenie będzie można zarządzać z portu Ethernet dostępnego na panelu czołowym.

Moce nadajników radiowych

Ze względu na wysokie koszty utrzymania częstotliwości radiowych dla zestawianych linków wymaga się aby dla częstotliwości 23, 18GHz moce nadajników radiowych dla modulacji 128QAM wynosiły nie mniej niż odpowiednio: 22 i 23 dBm dla 23 i 18GHz.

Router sieci utrzymaniowej

Urządzenie wyposażone musi być we wbudowany router DCN pracujący z protokołami TCP/IP i OSPF.

Konfiguracje sprzętowe

Oferowany system radioliniowy powinien umożliwiać realizowanie konfiguracji 1+0. Część wewnątrz-budynkowa (IDU) powinna składać się z pojedynczego modułu.

Radiolinia powinna mieć możliwość rozbudowy do 1+1 w późniejszym okresie w tej samej obudowie urządzenia dostarczonego.

Pasmo radiowe

Oferowany sprzęt radioliniowy powinien pracować w modulacji QPSK oferując pasmo dla styku radiowego o szerokości 3,5, 7, 14 i 28MHz poprzez softwarową zmianę konfiguracji.

Częstotliwości radiowe

Oferowane przęsło radioliniowe powinno pracować w paśmie 23GHz z antenami o średnicy 0,6m lub 1,2m. Oprócz powyższego pasma dany system powinien posiadać możliwość pracy w zakresie częstotliwości 6, 7, 8, 10.5, 11, 13, 15, 18, 26, 28, 32, 38GHz. Zmiana pasma pracy

odbywa poprzez zmianę modułu radiowego, anteny oraz programowego przełączenia przepływności w modemie radiowym.

Moduły radiowe powinny być zintegrowane z antenami o wymiarach 0,3m, 0,6m, 1,2m, 1,8m. Dla anten powyżej 1,8m dopuszcza się oddzielny montaż anten i modułów radiowych połączonych ze sobą falowodem.

System zarządzania

Każdy terminal powinien być wyposażony w konfigurator (LCT).

Każdy terminal powinien oferować możliwość wysyłania alarmów po SNMP wprost z urządzenia.

Nowe wersje oprogramowania

System zarządzania powinien oferować następujące możliwości uaktualniania oprogramowania:

- Uaktualnienie lokalne polegające na wgrywaniu nowego oprogramowania z konfiguratora dołączonego bezpośrednio do urządzenia
- Uaktualnienie zdalne, polegające na wgrywaniu nowego oprogramowania z centrum zarządzania siecią.
- Mechanizm wgrywania oprogramowania powinien wykorzystywać protokół FTP.

Zachowywanie konfiguracji

Każdy terminal powinien oferować możliwość zgrywania swojej konfiguracji na wskazany zewnętrzny serwer dostępny przez sieć utrzymaniową. Mechanizm zgrywania konfiguracji powinien wykorzystywać protokół FTP.

Odtwarzanie konfiguracji

Każdy terminal powinien oferować możliwość odtworzenia swojej konfiguracji. Mechanizm odtwarzania konfiguracji powinien wykorzystywać protokół FTP, poprzez który terminal radioliniowy będzie w stanie połączyć się w zewnętrznym serwerem FTP i pobrać ze wskazanego miejsce odpowiedni plik konfiguracyjny. Połączenie z serwerem FTP powinno być realizowane lokalnie lub przez sieć utrzymaniową.

2.3. Wymagania minimalne dla systemu zarządzania siecią

Wykonawca dostarczy oprogramowanie do zarządzania siecią spełniający niżej określone wymagania. Wykonawca udzieli Zamawiającemu bezterminowej licencji na korzystanie z dostarczonego oprogramowania. Ponadto wykonawca:

- Zainstaluje oprogramowanie systemu we wskazanym przez Zamawiającego środowisku sprzętowo – systemowym,
- Skonfiguruje sieć dla usług świadczonych przez Zamawiającego poprzez sieć,
- Skonfiguruje serwer monitoringu i logów (naniesienie wszystkich urządzeń i zintegrowanie ich z systemem),
- Naniesie istniejące urządzenia do systemu monitoringu.

Lp.	Obszar	Wymagania
1	**Zarządzanie użytkownikami**	• udostępnianie i podział łącza w sposób dynamiczny (realizowany przez algorytm kolejkowania) lub statyczny • wybór algorytmu kolejkowania pomiędzy HFSC i HTB

		• wybór metody kolejkowania w kolejkach głównych, usługowych oraz kolejkach użytkowników (dostępne metody to PFIFO, SFQ, ESFQ lub SRR) • limitowanie ilości połączeń każdego użytkownika sieci • możliwość grupowania klientów (kilka IP do wspólnej kolejki o określonej prędkości) • możliwość "przyspieszenia" ruchu www poprzez skierowanie do odrębnej, szybkiej kolejki usługowej z limitem do określonej wielkości jednorazowo pobranych danych dla każdej sesji • możliwość "przyspieszenia" początkowego ruchu w ramach kolejki użytkownika (prędkość kolejki klienta może być przez kilka początkowych sekund wyższa od standardowej prędkości danego klienta) • zaawansowana możliwość ustalania sposobu podziału (z priorytetowaniem usług lub wyłącznie "na klientów") • przydzielanie (indywidualnie każdemu z użytkowników sieci lokalnej) gwarantowanej i maksymalnej szybkości transferu danych z i do Internetu • dzielenie łącza z możliwością dodatkowego podziału i ustawienia wyższego priorytetu dla wskazanych portów bezpośrednio w ramach kolejki użytkownika • możliwość ustalenia różnych przydziałów prędkości dla klientów na dzień i w nocy (dwie taryfy) • blokada ruchu klienta o określonych godzinach lub dniach tygodnia • zaawansowane limitowanie oraz blokowanie ruchu programów p2p (także w wybranych godzinach lub dniach tygodnia) • blokada prób ruchu p2p na określonych portach lub zakresie portów • limitowanie ilości wykrytych połączeń p2p każdego użytkownika sieci (jednoczesnych połączeń oraz ilości połączeń na sekundę - zarówno tcp, jak i udp) • zaawansowana konfiguracja blokowania portów dla ruchu internetowego klientów sieci (także z użyciem celu NOTRACK i w tablicy raw) • limitowanie wielkości transferu w MB lub GB dla dowolnego okresu czasu z funkcją zapisywania liczników • zabezpieczenie przed skanowaniem portów i nieautoryzowanym dostępem do usług serwera • ochrona przed atakami Denial of Service (DoS), ICMP Flood, Syn Flood, Ping of Death i innymi rodzajami ataków • skuteczne blokowanie klientów rozsyłających SPAM wraz z logowaniem informacji o nich • podstawowe zabezpieczenie dostępu do sieci lokalnej oraz internetu wg adresów sprzętowych (MAC) kart sieciowych klientów • zabezpieczenie przed dalszym udostępnianiem internetu przez klientów w sieci lokalnej • skuteczne zabezpieczenie serwera przed dostępem niepożądanych połączeń i nieuprawnionych osób zarówno od strony internetu (firewall filtr stateful-inspection), jak i sieci lokalnej (bogate opcje konfiguracyjne) • wyłączenie z ruchu błędnych i fałszywych pakietów oraz ruchu niektórych wirusów • możliwość przekierowania ruchu www (transparent proxy) na router lub inny serwer w sieci lokalnej • możliwość przekierowania dowolnego ruchu na inny serwer lub port • zaawansowane przekierowanie wybranych portów lub publicznych adresów IP na komputer w sieci lokalnej (z możliwością limitowania ilości połączeń) • wyświetlanie komunikatów w przeglądarkach www klientów w sieci lokalnej (np. przypomnienie o zapłacie abonamentu itp.) • jednorazowe komunikaty "za potwierdzeniem" (z informacją o dacie i godz. odczytu) lub komunikaty wyświetlane cyklicznie • możliwość włączenia usługi "wizytówka sieci", która umożliwia wyświetlenie strony np. z treścią reklamową i danymi kontaktowymi dostawcy internetu dla nowych klientów sieci WiFi • łatwa edycja powiadomień, komunikatów i strony "wizytówki sieci" z użyciem edytora WYSYWIG • generowanie indywidualnych statystyk ruchu każdego użytkownika sieci (4

		wykresy z różnych przedziałów czasowych) • dostęp do szczegółowych statystyk obciążenia procesora, pamięci oraz interfejsów sieciowych routera • generowanie ogólnego wykresu wykorzystania usług sieciowych z podziałem na protokoły: http, ssl, ftp, smtp,pop3, imap, sip • logowania informacji o połączeniach internetowych klientów w sieci z automatyczną archiwizacją plików zawierających te informacje (realizuje ustawowy obowiązek dostawcy Internetowego) • innowacyjna możliwość wykonania kolejkowania po stronie WAN lub LAN, z użyciem interfejsów wirtualnych IMQ lub tylko na interfejsach fizycznych • możliwość samodzielnej edycji i zmian wielu elementów oprogramowania przez zaawansowanych administratorów (bezpośrednia edycja części kodu oprogramowania) • kontrola i edycja ustawień zarówno poprzez konsolę tekstową, jak i autorski panel administracyjny www w PHP • możliwość włączenia autoryzacji przez formularz www SSL lub PPPoE - dla wszystkich lub tylko dla części klientów sieci • automatyczny backup konfiguracji oraz możliwość szybkiego i łatwego exportu, bądź importu konfiguracji serwera poprzez FTP (obsługa z poziomu panelu administracyjnego) • monitorowanie wybranych urządzeń sieciowych z funkcją automatycznego logowania, powiadamiania o awariach na konto komunikatora gadu-gadu oraz via e-mail
2	**Monitoring**	• Graficzny interfejs podglądu Sieci z poziomu www • Przedstawienie wszystkich elementów Sieci w na mapie graficznej • Podgląd wszystkich logów urządzenia w systemie • Zbieranie logów i zapisywanie w bazie danych • Możliwość naniesienia na mapę innych urządzeń • Możliwość naniesienia na mapę przebiegów tras kabli światłowodowych • Możliwość naniesienia na mapę innych urządzeń aktywnych w Sieci • Możliwość odczytywania i zbierania logów (SNMP) z innych urządzeń aktywnych • Możliwość dynamicznego ustawiania czasu sprawdzania urządzeń • Możliwość testowania urządzeń po ICMP, WWW, TELNET, SSH • Wizualny komunikat o krytycznym błędzie urządzenia • Wizualny komunikat o krytycznym błędzie węzła • Powiadomienie sms • Powiadomienie email
3	**Główne cechy oprogramowania**	• Zaawansowana kontrola pasma - QoS • Zaawansowany firewall, obsługa tuneli i kodowania IPsec • STP bridging with filtering capabilities • Wysoka prędkość połączeń bezprzewodowych 802.11a/b/g z kodowaniem WEP • Obsługa WDS i Virtual AP • Obsługa HotSpot dla łatwego dostępu bezprzewodowego klientów • Obsługa protokołów RIP, OSPF, BGP • Obsługa kart Gigabitowych • Obsługa V.35, X.21, T1/E1 • Połączenia PPP z RADUIS AAA • Telefonia IP • Zdalna administracja winbox GUI • Konfiguracja za pomocą telnetu, ssh lub portu szeregowego

		• Konfiguracja i monitorowanie w czasie rzeczywistym

3. Stacje przekaźnikowe (min. 26 szt.)

Wykonawca zobowiązany jest do przygotowania dokumentacji niezbędnej do uzyskania pozwoleń na budowę lub zgłoszeń robót budowlanych związanych z budową masztów lub zgłoszeń i zainstalowania stacji przekaźnikowych zgodnie z projektem sieci. Wykonawca zobowiązany jest zastosować maszty kratownicowe w przypadku konieczności budowy masztów wyższych niż 3 m.

Po ukończeniu budowy każdej stacji przekaźnikowej Wykonawca zobowiązany jest do wykonania dokumentacji powykonawczej zgodnej z projektem sieci i wykonania zdjęcia każdej zainstalowanej stacji przekaźnikowej wraz z widocznym masztem i całym budynkiem.

Każda stacja przekaźnikowa składać się będzie z jednostki abonenckiej systemu WiMAX/LMDS i punktów dostępowych WiFi.

a) Wymagania minimalne dla jednostek abonenckich systemu WiMAX:

- Składające się z części zewnętrznej ODU montowanej na maszcie (ze zintegrowaną anteną obu polaryzacji lub ze złączem do przyłączenia osobnej anteny) oraz części wewnętrznej IDU instalowanej wewnątrz budynku lub w obudowie stacji bazowej WI-FI.
- możliwość pracy w czterech trybach (802.16d i e, TDD i FDD)
- obsługa całego podpasma 3.4-3.6 lub 3.6-3.8GHz
- możliwość pracy zarówno z polaryzacją pionową jak i poziomą
- możliwość wyboru jednostek abonenckich ze zintegrowaną anteną lub z anteną zewnętrzną o większym zysku
- możliwość przełączania się do sąsiednich sektorów lub stacji bazowych w przypadku braku sygnału radiowego z aktualnie obsługującego ją sektora/stacji bazowej
- możliwość fizycznej i logicznej integracji z punktem dostępowym Wi-Fi zewnętrznym
- możliwość fizycznej i logicznej integracji z punktem dostępowym Wi-Fi wewnętrznym
- jednostka abonencka powinna być połączona z urządzeniami końcowymi klienta za pomocą kabla sieciowego kategorii 5e
- możliwość jednoczesnej transmisji danych i prowadzenie połączeń głosowych
- możliwość zarządzania zdalnego za pomocą centralnego systemu nadzoru, jak i lokalnego za pomocą komputera typu PC podłączonego do jednostki abonenckiej
- przeźroczystość 512 adresów MAC
- gniazdo IEEE 802.3 Ethernet 10/100 BaseT
- zintegrowana antena 17 dBi
- możliwość podłączenia zewnętrznego miernika sygnału
- konfiguracja z poziomu www lub telnet
- obudowa zewnętrzna hermetyczna
- modulacja od QAM64 do BPSK(8 poziomów)
- maksymalna moc 20dbm
- pasma kanałów: 1.75MHz, 3.5MHz, 5MHz, 7MHz, 10MHz
- temperatura pracy: w warunkach zewnętrznych
- zasilanie 230 VAC
- ATPC
- QoS

- jednostka abonencka powinna posiadać certyfikat WiMAX Forum (jeśli WiMAX Forum określiło profil systemu w danym paśmie)
- jednostka abonencka nie powinna posiadać ograniczenia sprzętowego i programowego dla przesyłanej przepustowości (brak ograniczenia przepustowości).

b) Wymagania minimalne dla jednostek abonenckich systemu LMDS:

- Montaż w racku 19”
- wyposażenie w urządzenie nadawczo-odbiorcze do transmisji radiowej
- możliwość umieszczenia nadajnika radiowego w odległości co najmniej 100 m od stacji bazowej
- Interfejsy E1 (min. 4)
- Interfejsy Ethernet 10/100 (min.2)
- Lokalny port konsoli
- zasilanie 230VAC lub 48 VDC
- wymagana funkcja analizy widma

c) Wymagania minimalne dla punktów dostępowych WiFi:

	Obszar wymagań	**Wymagania minimalne**
	Płyta główna	– Procesor - 300MHz – Pamięć - 64MB DDR SDRAM – Dysk - 64MB pamięci NAND na stałe wbudowane w płytę – Port LAN - 3x10/100 Mbit/s Fast Ethernet port z obsługą Auto-MDI/X – Sloty miniPCI - 3x MiniPCI Typ IIIA/IIIB – Port szeregowy - jeden DB9 RS232C, standardowo 115200bps 8N1 – Zasilanie - pasywne PoE 10V do 28V DC lub gniazdo zasilające DC – Zasilacz w komplecie
	Karta 2,4/5GHz w standardzie 802.11a+b+g sztuk 2 dla każdego zestawu	**Podstawowe cechy:** – Turbo, 802.11a, 802.11b/g w jednej karcie – Pracuje w obu 2.4 and 5Ghz pasmach – Zwiększony zasięg dzięki mocniejszemu sygnałowi wyjściowemu – Zgodna z CE i FCC – Pracuje w zakresie 2.192-2.539 oraz 4.920-6.100GHz i obsługuje tryb Turbo. **Dane techniczne:** – Chipset: Atheros AR5414 lub równoważny – Standards: IEEE802.11a/b/g – Media Access: CSMA/CA with ACK architecture 32-bit MAC – Security: 64/128bit WEP, TKIP and AES-CCM encryption, WPA,WPA2, 802.1x – Modulation: 802.11b+g DSSS, OFDM for data rate >30Mb and for 802.11a – Interface: Mini-PCI form ver1.0 type 3B – Connectors: 2x uFl – Frequencies: 2.192-2.539 and 4.920-6.100GHz – Output Power/Sensitivity: 802.11a - 24dBm/-90dBm@6Mbps, 19dBm/-70dBm@54Mbps 802.11b - 25dBm/-92dbm@1Mbps, 25dBm/-87dBm@11Mbps 802.11g - 25dBm/-90dBm@6Mbps, 20dBm/-70dBm@54Mbps
	Obudowa	– wykonanie obudowy - odlew aluminiowy malowany proszkowo – klasa szczelności IP65 (uszczelka)
	Konektor uFl->N gniazdo 6Ghz 30cm sztuk 2 dla każdego zestawu	Konektor długości 30cm, kabla RG178. Z jednej strony subminiaturowe złącze uFl. Z drugiej strony N gniazdo, pozwalające na zamocowanie w obudowie.

	System Operacyjny	**Funkcje bezprzewodowego punktu dostępowego** – Access Point i klient – WDS i Virtual AP – 802.11a, 802.11g z prędkością do 108Mbps; wsparcie dla 802.11b – szyfrowanie WEP z kluczem 40 lub 104 bitowym – ACL (access controll list) i autentykacja RADIUS **Podstawowe cechy systemu** – Kształtowanie ruchu z wykorzystaniem HTB – Ograniczanie ruchu generowanego przez protokoły P2P (Kazaa, Direct Connect i inne) – DNS caching – HTTP proxy – Virtual Router Redundancy Protocol (VRRP) – Firewall i NAT – DMZ – IPsec, tunelowanie VPN (PPTP, L2TP, EoIP, IPIP), VLAN, PPPoE – Mosty STP z filtrowaniem pakietów – Equal cost multi path routing – Policy based routing **Funkcjonalność "Plug and Play"** – HotSpot z autentykacją RADIUS – Uniwersalny Klient – DHCP - serwer i relay – Protokół Univesal Plug and Play (UpnP) – Protokoły RIP, OSPF i BGP **Zarządzanie** – Poprzez terminal znakowy, specjalnym zestawem komend – Zdalnie, poprzez interfejs graficzny – Aktualizacja poprzez TFTP – Możliwość tworzenia skryptów – Zarządzanie z wykorzystaniem SNMP ACL (access controll list) i autentykacja RADIUS **Ograniczenia licencji:** – liczba tuneli PPPoE, PPTP, L2TP - 200 – liczba jednocześnie obsługiwanych klientów Hot-Spot - 200
	Antena 2,4 GHz – dookólna	**Dane techniczne:** – częstotliwości pracy: 2,4-2,48 GHz – zysk energetyczny minimum 17dBi – polaryzacja fali - pozioma – kąt promieniowania w płaszczyźnie poziomej- 360° z – odchyleniem od średniego zysku w granicach max 2dB (liść koniczyny) – kąt promieniowania w płaszczyźnie pionowej - 12°
	Antena 5,5 GHz – dookólna	– częstotliwość: 5450-5850MHz – impedancja: 50 ohm – VSWR: < 2.0 – Polaryzacja pionowa – Zysk: minimum 12dBi – szerokość wiązki (-3dB): pozioma: 360° – szerokość wiązki (-3dB): pionowa: 6°

		– ochrona elektryczna: zwarta dla prądu stałego
	Konektor 1 metr Nwtyk – Nwtyk sztuk 2 do każdego zestawu	– kabel MRC400 – złacza Nwtyk zaciskane
	Zasilacz buforowy	– Napięcie wejściowe 90-230V AC / 90-350V DC – Moc znamionowa 150W – Prąd wyjściowy 4A + 2A ładowanie akumulatora – Napięcie wyjściowe 25V +/- 5% – Min. poj. akumulatorów 5Ah – Napięcie akumulatorów 24V nominalnie – Zabezpieczenie zwarciowe

4. Urządzenia odbiorcze WiFi (120 szt.)

Wykonawca dostarczy i zainstaluje w gospodarstwach domowych beneficjentów ostatecznych urządzenia odbiorcze WiFi (klienckie). Lista beneficjentów ostatecznych zostanie przekazana Wykonawcy po zakończeniu rekrutacji.

Urządzenie klienckie zintegrowane z anteną na 5GHz., moc 24dBm radio oraz antenę 14dB o podwójnej polaryzacji. konfiguracja z poziomu WWW. Urządzenie powinno posiadać funkcję QoS. Pozostałe wymagania minimalne:

- procesor: minimum 180MHz
- pamięć: 16MB SDRAM, 4MB Flash
- interfejs ethernet: 1 X 10/100 BASE-TX (RJ-45)
- moc wyjściowa: minimum 24dBm, +/-2dB
- czułość radia: minimum -94dBm +/-2dB
- antena: minimum 14dBi, podwójna polaryzacja + zewn. wyjście RPSMA
- zasilanie PoE
- temp. pracy: w warunkach zewnętrznych
- Zasilacz oraz injector PoE.

5. Komputery z oprogramowaniem (120 szt.)

Zamawiający wymaga dostawy komputerów o następujących parametrach minimalnych:

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
1.	Płyta główna	Zaprojektowana przez producenta jednostki centralnej komputera, wyposażona w min. 2 sloty PCI i 1 slot PCI-Express x16 (ze wsparciem dla PCIe x1, dopuszcza się złącza Low Profile), 2 złącza DIMM, obsługa do 4GB pamięci RAM, kontroler SATA II (dla min. 2 urządzeń)
2.	Chipset	Dostosowany do oferowanego procesora min G31 lub równoważny
3.	Procesor	Procesor klasy x86, dedykowany do pracy w komputerach, taktowany zegarem co najmniej 2,60GHz, częstotliwość szyny systemowej min. 800MHz pamięć L2 2MB lub procesor równoważny wydajnościowo według wyniku testów przeprowadzonych przez Oferenta.
4.	Pamięć RAM	2GB DDR2 800MHz (2x1024MB)
5.	Dysk twardy	Min. 160 GB SATAII 7200rpm, 8MB pamięci Cache
6.	Karta graficzna	Zintegrowana, z możliwością dynamicznego przydzielenia pamięci w obrębie pamięci systemowej do min. 256MB, np. Intel GMA 3100 lub równoważna
7.	Karta dźwiękowa	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition (ADI 1984A
8.	Karta sieciowa	Wbudowana: 10/100/1000Mbit/s, Ethernet RJ 45, PXE 2.0, ASF 2.0
9.	Porty	Wbudowane: 1 x LPT; 1 x RS232, 1 x VGA; min. 8 x USB w tym min. 2 z przodu obudowy; wymagana ilość portów nie może być uzyskana poprzez stosowanie przejściówek lub kart PCI
10.	Klawiatura	Klawiatura USB w układzie polski programisty – trwale oznaczona logo producenta jednostki centralnej
11.	Mysz	Mysz laserowa USB z sześcioma klawiszami oraz rolką (scroll) min 1000dpi – trwale oznaczona logo producenta
12.	Napęd optyczny	Nagrywarka DVD +/-RW wraz z oprogramowaniem do nagrywania płyt
13.	System operacyjny	Microsoft Windows Vista HOME BASIC PL 32-bit z SP1, zainstalowany system operacyjny niewymagający aktywacji za pomocą telefonu lub Internetu w firmie Microsoft. Dołączony nośnik z oprogramowaniem
14.	Obudowa	– Konwertowalna (układ pracy pionowy i poziomy) w standardzie uBTX lub uATX, posiadająca min. 1 wnękę 5.25" i 1 wnękę 3.5" zewnętrzne oraz 1 wnękę 3.5" wewnętrzną (wnęki pełnej wysokości, nie dopuszcza się napędów typu slim) – Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń i napędów bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych);

		– 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) – Zasilacz o mocy max. 255W – W obudowę komputera musi być wbudowany wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami; a w szczególności musi sygnalizować: ▪ Przebieg procedury POST ▪ Sum kontrolnych BIOSu ▪ Awarii procesora lub pamięci podręcznej procesora ▪ Uszkodzenia lub braku pamięci RAM, uszkodzenia złączy PCI, kontrolera Video, dysku twardego, płyty głównej, kontrolera USB
15.	BIOS	- Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS) - Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń - Możliwość polegająca na kontrolowaniu urządzeń wykorzystujących magistralę komunikacyjną PCI, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych. Pod pojęciem kontroli Zamawiający rozumie funkcjonalność polegającą na blokowaniu/odblokowaniu slotów PCI. - Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na poziomie systemu, administratora oraz dysku twardego oraz możliwość ustawienia następujących zależności pomiędzy nimi: brak możliwości zmiany hasła pozwalającego na uruchomienie systemu bez podania hasła administratora. - Musi posiadać możliwość ustawienia zależności pomiędzy hasłem administratora a hasłem systemowy tak, aby nie było możliwe wprowadzenie zmian w BIOS wyłącznie po podaniu hasła systemowego. Funkcja ta ma wymuszać podanie hasła administratora przy próbie zmiany ustawień BIOS w sytuacji, gdy zostało podane hasło systemowe. - Możliwość odczytania z BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych , informacji na temat: zainstalowanego procesora, pamięci operacyjnej RAM wraz z informacją o obsadzeniu slotów pamięci, obsadzeniu slotów PCI. - Możliwość włączenia/wyłączenia zintegrowanej karty dźwiękowej, karty sieciowej, portu równoległego, portu szeregowego z poziomu BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. - Możliwość ustawienia portów USB w trybie „no BOOT", czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. - Możliwość wyłączania portów USB w tym: wszystkich portów, tylko portów znajdujących się na przodzie obudowy. - Możliwość zmiany trybu pracy dysku twardego: na pracę zapewniającą największą wydajność, na pracę zmniejszającą poziom hałasu generowanego przez dysk twardy. - Możliwość zablokowania zapisu na dyskietki
16.	Certyfikaty i standardy	– Certyfikat ISO 9001:2000 dla producenta sprzętu (do oferty należy załączyć kopie certyfikatu potwierdzającą spełnianie wymogu) – Certyfikat ISO 14001 dla producenta sprzętu (do oferty należy załączyć kopie certyfikatu potwierdzającą spełnianie wymogu) – Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z wymaganym systemem operacyjnym Vista (do oferty należy załączyć wydruk ze strony Microsoft) – Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie jałowym (IDLE) wynosząca maksymalnie 24dB (załączyć oświadczenie producenta wraz z raportem badawczym wystawionym przez niezależną akredytowaną jednostkę) – Deklaracja CE (należy załączyć do oferty dokument potwierdzający spełnienie

		wymogu) – Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia wykonawcy wystawionego na podstawie dokumentacji producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych", pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram – Certyfikat EPEAT na poziomie GOLD Wymagany wpis dotyczący oferowanego komputera w internetowym katalogu http://www.epeat.net - dopuszcza się wydruk ze strony internetowej
17.	Gwarancja na cały zestaw z monitorem	5-letnia gwarancja producenta świadczona na miejscu u klienta Czas reakcji serwisu - do końca następnego dnia roboczego. Gwarancja na sprzet orza oprogramowanie fabrycznie zainstalowane na komputerze. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem gwarancyjnym.
18.	Inne	Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Dołączony nośnik ze sterownikami.
	Wydajność komputera	Zamawiający ma prawo wezwać Oferenta do dostarczenia zaproponowanego komputera w celu weryfikacji spełnienia wymagań z SIWZ.

W cenie ofertowej należy uwzględnić:

- Dostarczenie zamówionych komputerów opisanych powyżej do miejsc użytkowania na terenie gmin uczestników projektu (zestawienie beneficjentów ostatecznych – użytkowników zostanie przekazane Wykonawcy po podpisaniu umowy),
- uruchomienie i konfigurację ww. urządzeń oraz oprogramowania,

W zestawie z komputerami wymagany jest pakiet oprogramowania antywirusowego, antyspamowego i firewall – dla każdego z dostarczonych komputerów o następujących parametrach minimalnych:

Lp.	Obszar wymagań	Wymagania minimalne
1.	Współpraca z systemem operacyjnym	Pełne wsparcie dla systemu Windows 2000/2003/XP/PC Tablet/Vista/2008. Wsparcie dla Windows Security Center (Windows XP SP2). Wsparcie dla 32- i 64-bitwej wersji systemu Windows. Wersja programu dla stacji roboczych Windows dostępna zarówno języku polskim jak i angielskim. Pomoc w programie (help) w języku polskim. Dokumentacja do programu dostępna w języku polskim. Skuteczność programu potwierdzona nagrodami VB100 i co najmniej dwie inne niezależne organizacje np. ICSA labs lub Check Mark.
2.	Ochrona antywirusowa i antyspyware	Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. Wbudowana technologia do ochrony przed rootkitami. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 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). Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie" i według harmonogramu. Możliwość skanowania dysków sieciowych i dysków przenośnych. Skanowanie plików spakowanych i skompresowanych. Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (w tym z uwzględnieniem plików bez rozszerzeń). Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu. 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. Wbudowany konektor dla programów MS Outlook, Outlook Express i Windows Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego). Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook. Skanowanie i oczyszczanie poczty przychodzącej POP3 "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. Możliwość definiowania różnych portów dla POP3, na których ma odbywać się skanowanie. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. Możliwość skanowania na żądanie lub według harmonogramu baz Outlook Express-a. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występujące w nawie strony. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie.. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów. Inkrementacyjne aktualizacje modułów analizy heurystycznej. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie powinny być wysyłane automatycznie, oraz czy próbki zagrożeń powinny być wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. Wysyłanie zagrożeń do laboratorium powinno być możliwe z serwera zdalnego zarządzania i lokalnie z każdej stacji roboczej w przypadku komputerów mobilnych. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń powinny być w pełni anonimowe.

		Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. Możliwość automatycznego wysyłania powiadomienia o wykrytych zagrożeniach do dowolnej stacji roboczej w sieci lokalnej. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e mail. Możliwość zabezpieczenia hasłem dostępu do opcji konfiguracyjnych programu. Możliwość zabezpieczenia hasłem możliwości wyłączenia programu antywirusowego i poszczególnych funkcji programu Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń. Aktualizacja dostępna z bezpośrednio Internetu, z lokalnego zasobu sieciowego, z CD ROM-u, oraz poprzez HTTP z dowolnej stacji roboczej lub serwera (moduł serwera HTTP wbudowany bezpośrednio w program). Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja). Możliwość określenia częstotliwości aktualizacji w odstępach 1 minutowych. Możliwość przypisania 2 profili aktualizacyjnych z różnymi ustawieniami do jednego zadania aktualizacji. Przykładowo, domyślny profil aktualizuje z sieci lokalnej a w przypadku jego niedostępności wybierany jest profil rezerwowy pobierający aktualizację z Internetu. Program wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, antyspam). Praca programu musi być niezauważalna dla użytkownika. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania.
3.	Ochrona przed spamem	Ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express i Windows Mail wykorzystująca filtry Bayes-a, białą i czarną listę oraz bazę charakterystyk wiadomości spamowych. Pełna integracja z programami pocztowymi MS Outlook, Outlook Express i Windows Mail – antyspamowe funkcje programu dostępne są bezpośrednio z menu programu pocztowego. Automatyczne wpisanie do białej listy wszystkich kontaktów z skrzynki adresowej programu pocztowego. Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną wiadomość i odwrotnie oraz ręcznego dodania wiadomości do białej i czarnej listy z wykorzystaniem funkcji programu zintegrowanych go z programem pocztowym.
4.	Zapora osobista (personal firewall)	Zapora osobista mogąca pracować jednym z 3 trybów: - tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące, - tryb interaktywny – program pyta się o każde nowe nawiązywane połączenie i automatycznie tworzy dla niego regułę (na stałe lub tymczasowo) - tryb oparty na zasadach – użytkownik/administrator musi ręcznie zdefiniować reguły określające jaki ruch jest blokowany a jaki przepuszczany. Możliwość tworzenia list sieci zaufanych. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokółu, aplikacji i adresu komputera zdalnego. Możliwość wyboru jednej z 3 akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj o decyzję. Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń. Możliwość zdefiniowania 2 oddzielnych zestawów reguł – jeden dla strefy zaufanej (sieć wewnętrzna) i drugi niezaufanej (internet). Wbudowany system IDS. Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu.
5.	Zdalna konsola administracyjna	Centralna instalacja i zarządzanie wszystkimi programami na stacjach roboczych Windows i serwerach Windows. Zdalna instalacja wszystkich wersji programu na stacjach roboczych Windows NT/2000/XP Professional/PC Tablet/ Vista. Do instalacji zdalnej i zarządzania zdalnego nie jest wymagany dodatkowy agent. Na

		końcówkach zainstalowany jest sam program antywirusowy Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, oraz zaporą osobistą (tworzenie reguł obowiązujących dla wszystkich stacji) zainstalowanymi na stacjach roboczych w sieci korporacyjnej z jednego serwera zarządzającego Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych z opcją wygenerowania raportu ze skanowania i przesłania do konsoli zarządzającej. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie i skanerów rezydentnych). Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, adresów MAC, wersji systemu operacyjnego oraz domeny, do której dana stacja robocza należy. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub internetu. Możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych. Możliwość tworzenia grup stacji roboczych i definiowania w ramach grupy wspólnych ustawień konfiguracyjnymi dla zarządzanych programów. Możliwość importowania konfiguracji programu z wybranej stacji roboczej a następnie przesłanie (skopiowanie) jej na inną stację lub grupę stacji roboczych w sieci. Możliwość zmiany konfiguracji na stacjach i serwerach z centralnej konsoli zarządzającej lub lokalnie (lokalnie tylko jeżeli ustawienia programu nie są zabezpieczone hasłem lub użytkownik/administrator zna hasło zabezpieczające ustawienia konfiguracyjne). Możliwość uruchomienia serwera zdalnej administracji na stacjach Windows NT/XP/2000 oraz na serwerach Windows NT 4.0/2000/2003. Możliwość uruchomienia centralnej konsoli zarządzającej na stacji roboczej Windows 98/ME/NT/2000/XP. Możliwość wymuszenia konieczności uwierzytelniania stacji roboczych przed połączeniem się z serwerem zarządzającym. Uwierzytelnianie przy pomcy zdefiniowanego na serwerze hasła. Do instalacji serwera centralnej administracji nie jest wymagane zainstalowanie żadnych dodatkowych baz typu MSDE lub MS SQL. Serwer centralnej administracji musi mieć własną wbudowaną bazę. Do instalacji serwera centralnej administracji nie jest wymagane zainstalowanie dodatkowych aplikacji takich jak Internet Information Service (IIS) czy Apache. Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) w formacie HTML lub CSV. Możliwość tworzenia hierarchicznej struktury serwerów zarządzających i replikowania informacji pomiędzy nimi w taki sposób, aby nadrzędny serwer miał wgląd w swoje stacje robocze i we wszystkie stacje robocze serwerów podrzędnych (struktura drzewiasta). Możliwość tworzenia repozytorium aktualizacji na serwerze centralnego zarządzania i udostępniania go przez wbudowany serwer http.

6. Wyposażenie serwerowni:

6.1 Oprogramowanie

Wykonawca dostarczy licencjonowane oprogramowanie:

A. do skanowania procesów systemowych, uruchomionych na komputerze, pozwalające oraz umożliwiające m.in. na:

I. okresowe skanowanie aktualnie uruchomionych procesów systemowych i informowanie administratora o wykrytych nieprawidłowościach. Moduł skanowania musi mieć możliwość skanowania całościowego (z zapisem do bazy danych) z możliwością okresowego skanowania z częstotliwością 24 godzin oraz różnicowego polegającego na zapisywaniu tylko nowo wykrytych procesów z możliwością okresowego skanowania z częstotliwością 1 godz.

II. Informacje o procesach zapisywane w bazie danych powinny zawierać następujące informacje: nazwa procesu, lokalizacja, zajmowana pamięć, nazwa

stanowiska gdzie po raz pierwszy wystąpił proces, data i czas wykrycia.

III. informowanie administratora poprzez e-mail o wszystkich nowych procesach otwartych na komputerze.

B. do nadzoru napędów wymiennych komputera, pozwalające oraz umożliwiające min. na:

I. zapisywanie w bazie danych informacji o:
   1. uruchamianiu komputera,
   2. kopiowaniu z/do urządzeń zewnętrznych typu: FDD, CDROM,USB

II. tworzenie raportów: kto, co, kiedy i gdzie kopiował i uruchamiał.

III. blokowanie kopiowania i uruchamiania z/do urządzeń zewnętrznych typu: FDD, CD-ROM, USB.

IV. autoryzacje wybranych urządzeń USB

C. do archiwizacji zasobów komputera, pozwalające oraz umożliwiające min. na:

I. tworzenie dowolnej ilości zadań w zakresie archiwizacji danych

II. zmiany parametrów zadań archiwizacji (ilość archiwów, kompresja, okres)

III. definiowanie rozszerzeń plików, które mają być pomijane podczas procesu archiwizacji oraz rozszerzeń plików np. *.doc, które mają być archiwizowane

IV. kopię całościową lub różnicową danych oraz przesyłanie plików z archiwizacji na wskazany serwer FTP

V. definiowanie cyklu archiwizacji

VI. wyświetlenie drzewa katalogów jakie zostały zarchiwizowane,zawartości ww. katalogów oraz możliwość odzyskania wcześniejszych wybranych kopii plików

VII. odzyskiwanie danych z wybranego okresu archiwizacji (wybór cyklu archiwizacji)

VIII. wyszukiwanie plików w utworzonych archiwach

IX. automatyczne usuwanie starszych plików kopii całościowej i różnicowej, definiowanie globalnego zadania archiwizacji

D. do inwentaryzacji komponentów komputerów, pozwalające oraz umożliwiające min. na:

I. okresową automatyczną inwentaryzację parametrów sprzętowych stanowiska: HDD, RAM, CPU, karta sieciowa, system operacyjny,karta graficzna itp.

II. analizę sprzętową:

   1. płyty głównej w zakresie: model, producent, nr seryjny
   2. CPU w zakresie: nazwa, model, producent, częstotliwość,
   3. HDD w zakresie: numer seryjny dysku, numer seryjny partycji, rozmiar pamięci, wolna przestrzeń pamięci
   4. RAM w zakresie: wielkość pamięci,
   5. karty sieciowej w zakresie: model, adres IP, adres MAC,
   6. karty graficznej w zakresie: model

III. odczyt informacji dotyczących systemu operacyjnego w zakresie: nazwa, wersja, data instalacji, zainstalowane poprawki, klucz licencyjny, produkt ID.

IV. odczyt informacji sieciowych w zakresie: adres IP, adres MAC, nazwa sieciowa.

V. odczyt informacji sprzętowych z BIOS w zakresie: nazwa BIOS, data, producent.

VI. przegląd historii zmian parametrów sprzętowych komputerów

VII. globalny przegląd stanowisk komputerowych pod względem parametrów sprzętowo-

systemowych

VIII. przypisywanie do komputera skanów dotyczących faktur zakupu (dodawanie, wydruk)

IX. automatyczne wykrywanie zmian w konfiguracji sprzętowej komputerów

X. zapis dodatkowych informacji inwentaryzacyjnych dotyczących całego stanowiska komputerowego w zakresie:

1. numeru seryjnego komputera,
2. numeru seryjnego monitora,
3. numeru seryjnego drukarki
4. numeru seryjnego dowolnych urządzeń peryferyjnych

XI. wydruk kartoteki sprzętowej stanowiska komputerowego

E. do inwentaryzacji każdego oprogramowania zainstalowanego na komputerach, pozwalające oraz umożliwiające min. na:

I. okresową automatyczną inwentaryzację zainstalowanego na komputerach każdego oprogramowania

II. globalny przegląd wszystkich programów zainstalowanych na oferowanych komputerach

III. tworzenie zestawień zainstalowanych typów programów (freeware, shareware itp.)

IV. porównywanie ilości posiadanych licencji programów z ilościami zainstalowanymi

V. przegląd historii instalacji oprogramowania na oferowanym komputerze

VI. wykaz komputerów z zainstalowanym, dowolnie wybranym programem

VII. przypisywanie do zainstalowanego oprogramowania skanów faktur zakupu (dodawanie, wydruk)

VIII. tworzenie zestawień duplikatów kluczy licencyjnych dotyczących zainstalowanego oprogramowania na oferowanym komputerze

IX. tworzenie zestawień zainstalowanych systemów operacyjnych na oferowanych komputerach

X. przesyłanie raportu z archiwizacji oraz raportu oprogramowania (lista programów zainstalowanych na stacji, informacje odczytywane z rejestru systemowego) na wskazany adres e-mail

F. do zdalnego zarządzania komputerami, pozwalające oraz umożliwiające min. na:

I. przechwytywanie (podłączenie) pulpitu wybranego użytkownika i/lub pulpitu grupy wybranych stanowisk użytkowników poprzez administratora za pomocą dedykowanej aplikacji do zdalnego zarządzania

II. całkowita interakcję administratora z użytkownikiem, polegającą na podłączeniu do stanowiska administratora stanowiska użytkownika, bez konieczności uprzedniego wylogowywania użytkownika. Oprogramowanie musi umożliwiając administratorowi dokonanie wyboru, kto posiada kontrolę nadrzędną nad sterowaniem pulpitem, administrator czy użytkownik.

III. szyfrowanie połączenia z użytkownikiem (min. algorytm AES 256 bitów lub równoważny, musi istnieć możliwość definiowania różnych kluczy szyfrujących dla różnych stanowisk/grup użytkowników)

IV. konfigurację przez administratora parametrów połączenia z użytkownikiem w zakresie: ilość kolorów, ilość klatek/sekundę, ukrywanie kursora myszy, skalowanie okna użytkownika jeżeli jest ono większe niż rozdzielczość stacji administratora.

V. przesyłanie plików/katalogów od zdalnego użytkownika do administratora i/lub od

administratora do zdalnego użytkownika.

VI. zarządzanie połączeniami z użytkownikami poprzez dodatkowy manager podłączania zdalnych pulpitów użytkowników, rezydujący na stacji administratora, w formie widocznej lub ukrytej zakładki na ekranie.
VII. zdalną dwukierunkową linie poleceń
VIII. zdalne zarządzanie kontami użytkowników w zakresie (tworzenie , usuwanie , edycja , zmiana hasła oraz typ konta)
IX. wysyłanie polecenia Wake-on lan

G. do nadzoru nadzoru WWW i aplikacji:

I. zestawienie najpopularniejszych adresów (jakie stanowiska je wywoływały, kiedy),
II. zestawienie najaktywniejszych stanowisk (pod kątem WWW), jakie adresy odwiedzały, kiedy,
III. podział stron na dozwolone i zabronione,
IV. wydruki tabelaryczne oraz graficzne (wykresy aktywności),
V. statystka aktywności stron WWW oraz aktywności stanowisk,
VI. blokada stron www (biała i czarna lista adresów, blokada pełna lub selektywna),
VII. analiza uruchamianych aplikacji (aktywność stanowisk, wykorzystanie zainstalowanych aplikacji),
VIII. filtracja okresowa oraz wg. grup stanowisk,
IX. wszystkie zestawienia do poziomu : Grupa\Stanowisko\Zalogowany Użytkownik.

H. do zapanowania nad awariami sprzętu:

I. Możliwość zgłoszenia przez użytkownika z poziomu przeglądarki WWW awarii sprzętu, usług, problemu z oprogramowaniem i innych typów awarii zdefiniowanych przez administratora.
II. Wykorzystanie bezpiecznego protokołu HTTPS.
III. Kontrola obciążenia działu IT (raporty ilości usuniętych usterek, statystyki pracy inżynierów oraz najczęściej pojawiających się awarii), optymalizacja podziału pracy pomiędzy pracowników działu IT oraz przegląd awaryjności sprzętu.
IV. Możliwość uwierzytelniania użytkowników wykorzystując bazę Active Directory poprzez protokół LDAP.
V. Możliwość autoryzowania określonych stanowisk i użytkowników, aby uniknąć każdorazowego uwierzytelniania przed korzystaniem z systemu zgłoszeń.
VI. Możliwość wprowadzenia przez użytkownika kilku awarii za jednym zgłoszeniem.
VII. Sortowanie listy zgłoszeń awarii, wg daty zgłoszenia, priorytetu, statusu.
VIII. Filtracja zgłoszenia wg priorytetu oraz statusu zgłoszenia, stanowisk oraz inżynierów obsługujących zgłoszenia.
IX. Możliwość dodania przez administratora nowego wpisu historii, jak i możliwość zmiany statusu sprawy. Użytkownik także ma mieć możliwość dodania nowego wpisu do zgłoszonego problemu wraz ze zmianą statusu.
X. Statusy mają być ustalane przez administratora z zaznaczeniem, których statusów może używać użytkownik zgłaszający problem.
XI. Użytkownik może otrzymać pocztą elektroniczną powiadomienia o nowych wpisach, zmianie statusu.
XII. Wielopoziomowa lista kategorii zawierająca nazwę i opis kategorii. Zapisane przez administratora rozwiązania problemów powiązuje się z kategoriami i mają być wyświetlane użytkownikom podczas przeglądania kategorii problemów. Rozwiązania mają posiadać znacznik określający czy są dostępne dla użytkowników, czy są wewnętrznymi uwagami działu IT.

XIII. Administrator ma mieć możliwość wprowadzenia problemu użytkownika, który nie ma dostępu do PC (np. telefonicznie informuje, że zepsuł mu się komputer).
XIV. Możliwość delegowania zgłoszenia innemu administratorowi (technikowi), jak również przejęcie innego zgłoszenia (np. w przypadku nieplanowanej nieobecności technika).
XV. Baza umów serwisowych powiązana z bazą firm serwisowych (dostawców sprzętu, oprogramowania, lokalnych serwisów). Możliwość powiązania każdej umowy z zakupionymi licencjami oprogramowania lub z zakupionym sprzętem.
XVI. Informowanie pracowników o przestojach serwera, awariach za pomocą komunikatów wprowadzanych na stronę główną panelu zgłaszania usterki, bądź do poszczególnych kategorii.

Dodatkowe wymagania:

I. dostęp do konsoli zarządzającej zabezpieczony fizycznym kluczem HASP wraz z hasłem dostępowym
II. możliwość pracy w konsoli wielu Administratorów jednocześnie z możliwością zarządzania prawami do poszczególnych modułów (zapis, edycja, odczyt, zarządzanie)
III. możliwość przypisania wybranych grup stanowisk do poszczególnych kluczy HASP (użytkowników konsoli). Wszelkie raporty, zestawienia oraz funkcje grupowe obejmują wtedy tylko w/w przypisane grupy.
IV. możliwość wykonywania audytu sprzętu oraz oprogramowania na stanowiskach nie podłączonych do sieci (export pliku)
V. możliwość dodawania skanów ręcznych (np. sprzęt uszkodzony, bez systemu operacyjnego)
VI. szyfrowana baza danych (na poziomie tabel tzn. każda tabela posiada inny klucz szyfrujący)
VII. współpraca z serwerem Firebird oraz MsSQL Server.
VIII. automatyczne wykrywanie zmian w konfiguracji sprzętowo-systemowej stanowisk (np. inny dysk twardy, karta graficzna, wielkość RAM)
IX. Ww. aplikacja w zakresie modułu zdalnego zarządzania musi pracować w formie usługi systemowej oraz musi być aktywna podczas przelogowywania użytkowników oraz przed zalogowaniem użytkownika do stacji.

6.2 Serwery (szt. 2)

Obudowa	Maksymalnie 2U do instalacji w standardowej szafie RACK 19", dostarczona wraz z szynami i prowadnicą kabli.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów, dwu lub czterordzeniowych, umożliwiająca przepustowość do 25 GB/s. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Dwa procesory czterordzeniowe klasy x86 dedykowane do pracy w serwerach zaprojektowane do pracy w układach dwuprocesorowych, taktowane zegarem co najmniej 2.4GHz, pamięć cache L3 8 MB lub procesor równoważny wydajnościowo według wyniku testów przeprowadzonych przez Oferenta. W przypadku zaoferowania procesora równoważnego Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testów oferent musi dostarczyć zamawiającemu oprogramowanie testujące, oba równoważne porównywalne zestawy oraz dokładny opis użytych testów

	wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od zamawiającego.
RAM	16 GB DDR3 1066 MHz, rejestrowana możliwość rozszerzenia do 192GB, na płycie głównej powinno znajdować się minimum 18 slotów przeznaczonych dla pamięci, możliwość instalacji kości pamięci RDIMM lub UDIMM.
Zabezpieczenia pamięci RAM	ECC, SBEC, SDDC (lub równoważny), Memory Mirror.
Gniazda PCI	Minimum 4 złącza PCI-E drugiej generacji w tym 2 x PCI-E x8 i 2 x PCI-E x4; Możliwość instalacji wymiennie modułu udostępniającego 1 x PCI-E x16 i 2 x PCI-Ex4
Interfejsy sieciowe	Minimum 4 porty typu 10/100/1000 wbudowane na płycie głównej z możliwością obsługi stosu TCP/IP – TOE, wsparciem dla protokołu IPv6 oraz możliwością obsługi iSCSI (w tym uruchamiania z iSCSI)
Napęd optyczny	Wewnętrzny napęd DVD-ROM
Dyski twarde	Możliwość instalacji dysków SATA, SAS lub SSD. Zainstalowane 2 dyski 73GB typu HotPlug SAS skonfigurowane jako RAID 1, możliwość instalacji minimum 6 dodatkowych dysków twardych Hot-Plug w obudowie serwera.
Kontroler RAID	Dedykowany kontroler RAID. Pamięć podręczna minimum 256MB, z podtrzymaniem bateryjnym, możliwe konfiguracje 0, 1, 10, 5, 50, 6, 60.
Porty	5 x USB 2.0 z czego 2 na przednim panelu obudowy, 2 na tylnym panelu obudowy i jeden wewnętrzny, 4 x RJ-45, VGA, 1 port szeregowy
Video	Zintegrowana karta graficzna, umożliwiająca rozdzielczość min. 1280x1024.
Elementy redundantne HotPlug	Min. Zasilacze, wentylatory, dyski twarde
Zasilacze	Wysokowydajne, redundantne, zasilacze Hot-Plug o mocy maksymalnie 870W każdy i typowej wydajności powyżej 91%, Wymagane dostarczenie raportu sporządzonego przez niezależną organizację.
Bezpieczeństwo	Zintegrowany z płytą główną moduł TPM, możliwość zainstalowania wewnętrznej karty pamięci SD oraz klucza USB.
Zarządzanie	Zintegrowany z płytą główną moduł zawierający sterowniki do systemów operacyjnych i oprogramowanie zgodne ze standardem UEFI umożliwiające: ▪ uaktualnienie przechowywanych sterowników i firmware'u urządzeń ▪ konfigurację kontrolera RAID ▪ instalację systemu operacyjnego bez konieczności korzystania z dodatkowej płyty ze sterownikami
Diagnostyka	Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Karta Zarządzania	Zintegrowana z płytą główną lub zainstalowana w dedykowanym slocie karta zarządzająca niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane złącze RJ-45 i umożliwiająca: ▪ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera) ▪ zdalny dostęp do graficznego interfejsu Web karty zarządzającej ▪ szyfrowane połączenie (SSLv3) oraz autentykacje i autoryzację użytkownika ▪ możliwość podmontowania zdalnych wirtualnych napędów ▪ wirtualną konsolę z dostępem do myszy, klawiatury ▪ wsparcie dla IPv6 ▪ wsparcie dla WSMAN (Web Service for Managament); SNMP; IPMI2.0, VLAN tagging, Telnet, SSH ▪ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer ▪ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer ▪ integracja z Active Directory

	▪ możliwość obsługi przez dwóch administratorów jednocześnie ▪ wsparcie dla dynamic DNS ▪ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej ▪ możliwość podłączenia lokalnego poprzez złącze RS-232
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001. Deklaracja CE. Serwer musi spełniać normy Energy Star 1.0 for Computer Servers. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Designed for Windows" dla MS Windows Server 2003 w wersji x86 i x64. Wymagane jest dostarczenie odpowiednich certyfikatów.
Warunki gwarancji	Przynajmniej trzy lata gwarancji z czasem reakcji w ciągu 4 godzin dla systemów o znaczeniu krytycznym, przyjmowanie zgłoszeń 24 godziny na dobę, 7 dni w tygodniu. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta serwera – dokumenty potwierdzające załączyć do oferty. Oświadczenie producenta serwera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. Zamawiający oczekuje fizycznej instalacji i testów uruchomieniowych oferowanych serwerów. Zamawiający oczekuje możliwości przedłużenia czasu gwarancji do pięciu lat.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

6.3 Macierz dyskowa (szt. 1)

Obudowa	Moduł podstawowy - maksymalnie 3U do instalacji w standardowej szafie RACK 19”
Kontrolery	Dwa kontrolery RAID pracujące w układzie active-active udostępniające łącznie minimum cztery złącza GigabitEthernet iSCSI do podłączenia serwerów. Wymagane poziomy RAID 0,1,5,10, niezależny dostęp do dysku każdego z kontrolerów. Wydajność macierzy min.60kIOPS
Cache	512MB na kontroler, pamięć cache zapisu mirrorowana między kontrolerami, z opcją zapisu na dysk lub podtrzymywana bateryjnie przez min. 72h w razie awarii
Dyski	Hot-Plug, FC lub SAS 5x300GB 15krpm, możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych, możliwość obsługi łącznie minimum 45 dysków.
Oprogramowanie	Zarządzające macierzą w tym powiadamianie mailem o awarii, umożliwiające maskowanie i mapowanie dysków. Upgrade bez zatrzymywania pracy macierzy. Możliwość wykonywania kopii migawkowych (min 8 per dysk wirtualny). Możliwość rozbudowania oprogramowania o funkcjonalność wykonywania pełnych kopii dysków logicznych, możliwość utworzenia minimum 128 LUN’ów Licencja macierzy powinna umożliwiać podłączanie minimum 16 hostów bez konieczności zakupu dodatkowych licencji dla macierzy.
Wsparcie dla systemów operacyjnych	MS Windows 2003 zarówno 32 jak i 64 bit, MS Windows 2008 Server, VMware ESX 3.5, wsparcie dla klastrów MS Windows 2003
Bezpieczeństwo	Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne, możliwość wymiany na gorąco bez zatrzymywania pracy macierzy.
Warunki gwarancji dla macierzy	Przynajmniej trzy lata gwarancji z czasem reakcji na rozpoczęcie naprawy maks. 4 godziny od zgłoszenia, dla systemów o znaczeniu newralgicznym, przyjmowanie zgłoszeń 24 godziny na dobę, 7 dni w tygodniu. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta serwera – dokumenty potwierdzające załączyć do oferty. Oświadczenie producenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. Zamawiający oczekuje instalacji macierzy z minimum 4 hostami. Zamawiający oczekuje możliwości przedłużenia czasu gwarancji do pięciu lat.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim
Certyfikaty	Macierz musi być wyprodukowana zgodnie z normą ISO 9001.

6.4 System operacyjny (szt. 2)

MS Windows Server Standard 2008

6.5 Zasilanie awaryjne (szt. 1)

- Minimalna moc pozorna : 6000VA
- Minimalna moc rzeczywista : 4200W
- Obudowa UPS'a dedykowana do montażu w szafie RACK

- Maksymalna wysokość : 3U
- Wymagania dodatkowe : Zimny start , sinus podczas pracy na baterii, automatyczna regulacja napięcia
- Gwarancja minimalnie 36 miesięcy.

6.6 Agregat prądotwórczy trójfazowy do zasilania serwerowni (szt. 1)

Agregat prądotwórczy o mocy znamionowej co najmniej 40 kVA, z silnikiem o zapłonie samoczynnym, stacjonarny, bez obudowy, z automatycznym rozruchem (układ samoczynnego załączania rezerwy automatycznie przełączający zasilanie pomiędzy siecią a zespołem przy braku napięcia z sieci, układ sterowania powinien zapewnić regulacje ostawień progów zadziałania i dokonywania przełączeń), wyposażony w podgrzewacz płynu chłodzącego, ze zbiornikiem na paliwo zapewniającym minimum 8 godz. pracy urządzenia pod obciążeniem znamionowym, chłodzony cieczą, wyposażony w licznik motogodzin; do pracy awaryjnej, fabrycznie nowy, z dostawą, rozładunkiem, instalacją we wskazanej lokalizacji, podłączeniem zasilania do wskazanych lokalizacji i uruchomieniem.

Minimalne parametry:
- Czas pracy na pełnym zbiorniku (godz.): min. 8
- Częstotliwość (Hz): 50
- Ilość faz: Trójfazowy
- Ilość pól prądnicy: 4
- Moc maksymalna (kVA) 40.0
- Moc nominalna (kVA) 37.0
- Napięcie (V): 230/400
- Paliwo: ON
- Podłączenie automatyki
- Silnik-typ: chłodzony cieczą, silnik Diesla
- System kontroli: Samokontrola i stabilizacja napięcia (AVR)
- System rozruchowy Elektryczny
- Zużycie paliwa (g/kWh) <300
- Dostawa ATS (Automatycznego systemu sterowania)

6.7 Zestaw komputerowy do administracji siecią dostępową (szt.1)

Lp	Nazwa	Opis wymaganych parametrów
1	Procesor	Dwurdzeniowy procesor mobilny minimum 1,6 GHz cache L2 3MB ze sprzętowym wsparciem technologii wirtualizacji
2	Płyta główna	Wspomagająca technologię wielowątkowości oraz dwurdzeniowości; Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, posiadająca sprzętowe wsparcie technologii wirtualizacji, wbudowany sprzętowy firewall, zarządzany i konfigurowany z serwera zarządzania oraz niedostępny dla lokalnego systemu OS i lokalnych aplikacji, a także umożliwiająca:

		a) monitorowanie konfiguracji komponentów komputera - CPU, Pamięć, HDD wersje, BIOS płyty głównej; b) zdalną konfigurację ustawień BIOS, c) zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego; d) zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nie ulotnej. e) nawiązywanie przez sprzętowy mechanizm zarządzania zdalnego szyfrowanego protokołem SSL/TLS połączenia z predefiniowanym serwerem zarządzającym, w definiowanych odstępach czasu, w przypadku wystąpienia predefiniowanego zdarzenia lub błędu systemowego (tzw. platform event) oraz na żądanie użytkownika z poziomu BIOS. f) wbudowany sprzętowo log operacji zdalnego zarządzania, możliwy do kasowania tylko przez upoważnionego użytkownika systemu sprzętowego zdalnego zarządzania
3	Chipset	Rekomendowany przez producenta procesora
4	Pamięć RAM	5GB DDR3 RAM
5	Kontroler HDD	Zintegrowany kontroler SATA (SSD)
6	HDD	Minimum HDD 128 GB półprzewodnikowy
7	Karta graficzna	Zintegrowana z możliwością dynamicznego przydzielenia do min. 256MB, ze sprzętowym wsparciem dla DirectX 10.0, Shader 4.0, Microsoft® Windows Vista™ Aero™
8	Wyświetlacz	12,1 WXGA rozdzielczość matrycy 1280x800 WLED (12.1-inch WXGA (1280x800) DLV WLED) , Technologia dotykowa,
9	Napęd optyczny	DVD-RW, dopuszcza się zewnętrzny napęd np. w dedykowanej stacji podpinanej pod złącze dokujące
10	Komunikacja	-zintegrowana karta sieciowa PCI Ethernet 10BaseT/100Base/1000 TX -WiFi IEEE 802.11a/b/g/n n (dedykowany przełącznik umożliwiający włączenie/wyłączenie łączności bezprzewodowej, czujnik pozwalający na znalezienie dostępnych sieci Wi-Fi bez konieczności uruchamiania komputera) umożliwiające zdalny dostęp do komputera z poziomu konsoli zarządzania - Bluetooth
11	Karta dźwiękowa	Zintegrowana karta dźwiękowa, głośnik wewnętrzny
12	BIOS	BIOS typu FLASH EPROM posiadający procedury oszczędzania energii i zapewniający mechanizm plug&play umożliwiający odczyt konfiguracji wraz z numerami seryjnymi (w tym numeru seryjnego komputera) przez sieć zgodny z DMI 2.0.

14	Porty I/O	Złącze RJ-45, 2 złącza USB 2.0, 1xUSB/eSATA, Express Card 34/54, wyjście VGA, czytnik kart SD, firewire IEEE1394, port złącza dokującego
15	Klawiatura	Klawiatura minimum 88 klawiszy
16	Waga	Nie więcej niz 2 kg z baterią 6-cell Dodatkowy moduł 45Wh
17	Zasilanie	Zewnętrzny zasilacz 220V 50Hz Bateria Li-Ion 6-cell czas pracy minimum 4 godziny. +zasilacz auto/air
18	Urządzenie wskazujące	Touchpad i trackPoint,
19	Obudowa	Współpraca z zabezpieczeniem antykradzieżowym typu Kensington Lock
20	Mechanizmy ochrony	Programowy, dwustopniowy system haseł na setup komputera
21	Oprogramowanie	-zainstalowany Windows 7 Professional PL z Service Pack 1 (64-bit) -komplet sterowników systemowych (na nośniku CD lub dostępny na stronie producenta)
22	Torba	Torba na tablet, akcesoria i dokumenty -wykonana z materiału wodoodpornego -posiadająca wzmocnienia zabezpieczające tablet przed uderzeniami
23	Inne	Gwarancja: 5 lat na miejscu u klienta. Czas reakcji serwisu - do końca następnego dnia roboczego Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. Uszkodzony dysk twardy pozostaje u Zamawiającego. 4 letnie ubezpieczenie sprzętu na wypadek min. upadku, kradzieży, zalania itp.
24	Dokumentacja	Dokumentacja użytkownika w języku polskim lub angielskim;
25	Zewnętrzna klawiatura i mysz	bezprzewodowa klawiatura w układzie QWERTY i bezprzewodowa myszą działająca na wielu powierzchniach, współpracujące z jednym, zgodnym odbiornikiem tego samego producenta
26	Monitor	Panel Lcd TN, Przekątna ekranu nie mniej niż 22" (56 cm), Technologia dotykowa optyczna, multitouch (2 kompatybilne punkty), aktywowany palcem lub rysikiem, w pełni kompatybilny z nowym systemem Windows® 7, Rozdzielczość: nie mniej niż Full HD (1920 x 1080). złącza: cyfrowe DVI-D (zgodne ze standardem HDCP) oraz analogowe D-Sub
27	Zewnętrzna karta sieciowa	Podłączana do komputera przez złącze USB 2.0, posiadająca zewnętrzne złącze anteny RP-SMA, posiadająca chipset pozwalający na włączenie trybu monitoringu i Packet Injection z poziomu systemu Windows

28	Drukarka	Druk w sieci na nośnikach wielkoformatowych do formatu A3+, technologia atramentowa, złącza: USB 2.0, Ethernet; liczba wkładów drukujących: 4 (czarny i trzy kolorowe)

6.8 Wyposażenie serwerowni oraz wykonane prace (szt. 1)

a) Wymagane jest dostarczenie szafy serwerowej o wymiarach szerokość min. 600mm, głębokość min. 1000mm , wysokość minimalnie 25U , kolor czarny.
b) Dostawa wszystkich niezbędnych elementów do uruchomienia dostarczonego sprzętu.
c) W obrębie sprzętu oraz Oprogramowania serwerowego od wykonawcy wymaga się :
   - Dostarczenia wymaganego sprzętu oraz licencji Oprogramowania do siedziby zamawiającego.
   - Kompletacji oraz fizycznego montażu w pomieszczeniu wskazanym przez zamawiającego.
   - Aktualizacji mikrokoków dostarczonego sprzętu do najnowszych wersji dostępnych u producenta.
   - Instalacji oraz konfiguracji wymaganego systemu operacyjnego.
   - Instalacji oraz konfiguracji środowiska wirtualnego z uwzględnieniem wszystkich funkcjonalności zawartych w dostarczonych licencjach.

6.9 Przeszkolenia administratora umożliwiającego przystąpienie do egzaminu Certyfikującego według zakresu : (szt. 1)

- instalacji serwerów wirtualnych
- Konfiguracji dostępu do sieci i dysków dla serwerów wirtualnych
- instalacji i konfiguracji konsoli zarządzającej
- kontroli dostępu do wirtualnej infrastruktury
- Zarządzania wirtualnymi maszynami
- alokacji i monitorowania zasobami wirtualnych maszyn
- zapewnienia wysokiej dostępności dla aplikacji
- rozwiązań typowych problemów związanych z serwerami wirtualnymi

6.10 Wymagania dotyczące licencji oprogramowania do wirtualizacji

Licencje powinny umożliwiać uruchomianie wirtualizacji na serwerach fizycznych o łącznej liczbie 4 procesorów oraz jednej licencji konsoli do zarządzania całym środowiskiem
Wszystkie licencje powinny być dostarczone wraz z rocznym wsparciem, świadczonym przez producenta oprogramowania, które powinno umożliwiać zgłaszanie problemów przez 5 dni tygodniu w godzinach od 06.00 do 18.00 .

Wymagania techniczne dot. oprogramowania

Konsolidacja

– Warstwa wirtualizacji powinna być rozwiązaniem systemowym tzn. powinna być zainstalowana bezpośrednio na sprzęcie fizycznym.

– Rozwiązanie powinno zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
– Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością dostępu do 255GB pamięci operacyjnej.
– Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1, 2, 3 i 4 procesorowych.
– Rozwiązanie powinno umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
– Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
– Rozwiązanie powinno wspierać następujące systemy operacyjne: Windows XP, Windows Vista , Windows NT, Windows 2000, Windows Server 2003, Windows Server 2008, SLES 10, SLES9, SLES8, Ubuntu 7.04, RHEL 5, RHEL 4, RHEL3, RHEL 2.1, Solaris wersja 10 dla platformy x86, NetWare 6.5, NetWare 6.0, NetWare 6.1, Debian, CentOS, FreeBSD, Asianux, Ubuntu 7.04, SCO OpenServer, SCO Unixware.
– Rozwiązanie powinno umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
– Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi usługami.
– Rozwiązanie powinno zapewnić możliwość monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej.
– Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii zapasowych instancji systemów operacyjnych oraz ich odtworzenia w możliwie najkrótszym czasie.
– Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
– Oprogramowanie do wirtualizacji powinno zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
– Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi Microsoft Active Directory.
– Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej z dwóch ścieżek.
– Platforma wirtualizacyjna musi umożliwiać wykorzystanie procesorów fizycznych do 12 rdzeni na procesor.
– Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych aniżeli fizycznie zarezerwowane.

Wysoka dostępność

– Rozwiązanie powinno mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi .
– Rozwiązanie powinno zapewnić ciągłą pracę usług. Usługi krytyczne biznesowo powinny działać bez przestoju, czas niedostępności innych usług nie powinien przekraczać kilkunastu minut.
– Powinna zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały przełączone na inne serwery infrastruktury.
– Rozwiązanie powinno umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury. Należy opisać wykorzystywany mechanizm.

– Rozwiązanie powinno zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania. Należy opisać wykorzystywany mechanizm.
– Rozwiązanie powinno zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej, hostowanych systemów operacyjnych (np. wgrywania patch-y) i aplikacji tak aby zminimalizować ryzyko awarii systemu na skutek wprowadzenia zamiany. Należy opisać wykorzystywany mechanizm.
– Rozwiązanie powinno zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych, niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii serwerów fizycznych, bez utraty danych i dostępności danych podczas awarii serwerów fizycznych.

– Rozwiązanie musi umożliwiać dodawanie i rozszerzanie dysków wirtualnych, procesorów i pamięci RAM podczas pracy wybranych systemów,
– System musi umożliwiać kontrole dostępu sieciowego do obszarów wrażliwych wirtualnego centrum danych takiego jak DMZ lub serwery z danymi wrażliwymi podlegające zgodności z przepisami PCI lub SOX w obszarze środowiska wirtualnego.

Równoważenie obciążenia i przestoje serwisowe

– Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) powinien być ograniczony do minimum. Pożądana jest możliwość przenoszenia usług pomiędzy serwerami fizycznymi bez przerywania pracy usług. Należy opisać wykorzystywany mechanizm.

Obsługa potrzeb biznesu

– Rozwiązanie powinno zapewnić mechanizm wykonywania kopii – klonów systemów operacyjnych wraz z ich pełną konfiguracją i danymi.

7. Serwis sieci i urządzeń

7.1. Serwis infrastruktury sieciowej

Wykonawca zobowiązany jest do utworzenia centrum zarządzania siecią, którego rolą będzie:
– monitorowanie sieci,
– usuwanie bieżących uszkodzeń infrastruktury sieciowej,
– raportowanie awarii (raporty powinny być dostępne z poziomu strony www),
– prowadzenie statystyk obciążenia elementów sieci (statystyki powinny być dostępne dla każdego użytkownika z poziomu systemu zarządzania siecią).

Wykonawca zobowiązany jest do świadczenia serwisu przez cały okres umowy.

Czas usunięcia awarii do 24 godz. od zdarzenia. Zwiększenie limitu czasu może nastąpić tylko w uzasadnionych przypadkach po pisemnym zgłoszeniu i akceptacji Zamawiającego.
Wykonawca zobowiązany jest do ubezpieczenia infrastruktury sieciowej od negatywnego wpływu czynników atmosferycznych przez cały okres serwisowania infrastruktury.

7.2. Serwis urządzeń u beneficjentów ostatecznych projektu

Wykonawca zobowiązany jest do zapewnienia wsparcia technicznego w formie infolinii 0801 + numer telefoniczny z strefy numeracyjnej 025 w dni robocze w godz.: 8:00 – 16:00.
Czas usunięcia awarii do 48 godz. od zgłoszenia. Zwiększenie limitu czasu może nastąpić tylko w uzasadnionych przypadkach po pisemnym zgłoszeniu i akceptacji Zamawiającego.
Wykonawca zobowiązany jest do ubezpieczenia urządzeń u beneficjentów końcowych od negatywnego wpływy czynników atmosferycznych przez cały okres serwisowania urządzeń.

8. Usługa dostępu do Internetu

Przedmiotem zamówienia w niniejszym postępowaniu jest świadczenie usługi nielimitowanego dostępu do Internetu na rzecz infrastruktury wybudowanej w ramach projektu przez okres: od momentu odbioru etapu: „Wyposażenie serwerowni" do 31.12.2012. Usługi świadczone będą w głównej lokalizacji sieci. Ponadto Wykonawca w ramach niniejszego zamówienia dostarczy odbiorcy router o parametrach technicznych umożliwiających korzystanie z usługi. Koszt dostarczenia, montażu i dzierżawy routera zostanie doliczony do abonamentu za świadczenie usługi.
Ponadto Wykonawca w ramach świadczonej usługi zapewni:

a) Stały dostęp do internetu;
b) Brak limitu transferu danych;
c) Nielimitowany czas dostępu do internetu;
d) Prędkość download co najmniej 20 Mb/s, maximum 25 Mb/s, upload co najmniej 20 Mb/s;
e) Pulę 256 stałych adresów IP (w jednej klasie C)
f) Wydajność gwarantowana 100% do i z routera brzegowego dostawcy

Abonament za świadczenie usługi dostępu do Internetu obejmuje wszelkie koszty związane z rozpoczęciem świadczenia usługi, w tym koszty montażu i dzierżawy niezbędnych urządzeń, ewentualne koszty dzierżawy łącz telefonicznych oraz koszty świadczenia usługi dostępu do Internetu, odpowiednio do oferowanego transferu. Zamawiający z tytułu rozpoczęcia świadczenia usług oraz świadczenia usług, za wyjątkiem abonamentu określonego w ofercie Wykonawcy, nie będzie ponosił żadnych dodatkowych opłat.

9. Promocja i informacja

Wykonawca ma obowiązek, na koszt własny, oznakować wszystkie dostarczone urządzenia i budowle trwałymi, niezdzieranymi i niezmywalnymi znakami graficznymi informującymi o dofinansowaniu programu ze środków Unii Europejskiej zgodnie z wytycznymi dotyczącymi promocji projektów finansowanych w ramach programu operacyjnego innowacyjna gospodarka. Znaki graficzne muszą zostać zaakceptowane przez Koordynatora prac występującego w imieniu Zamawiającego przed ich umieszczeniem na urządzeniach i budowlach.