



Załącznik nr 6 do SIWZ

Szczegółowy opis przedmiotu zamówienia



Spis treści:

1.	ZAŁOŻENIA	3
2.	WYMAGANIA	3
3.	CENTRUM SIECI	5
4.	ŁĄCZE INTERNETOWE	5
5.	SIEĆ ŚWIATŁOWODOWA	5
6.	OPIS PUNKTÓW DYSTRYBUCYJNYCH SIECI ŚWIATŁOWODOWEJ	8
7.	LOKALIZACJA STACJI BAZOWYCH	9
8.	ILOŚĆ SEKTORÓW, PODZIAŁ LOKALIZACJI POMIĘDZY SEKTORY	9
9.	STACJA BAZOWA – 5 SZT.....	9
10.	TERMINALE ABONENCKIE – 60 SZT.	11
11.	SYSTEM ZARZĄDZANIA SIECIĄ WIMAX – 1 SZT.	12
12.	SZKIELETOWE PRZEŁĄCZNIKI SIECIOWE – 2 SZT.....	13
13.	DYSTRYBUCYJNE PRZEŁĄCZNIKI SIECIOWE – 12 SZT.	17
14.	URZĄDZENIE ZABEZPIECZAJĄCE TYPU FIREWALL – 1 SZT.....	18
15.	MINIMALNE PARAMETRY TECHNICZNE SERWERA – 2 SZT.....	20
16.	ZASILACZ AWARYJNY UPS – 12 SZT.....	23
17.	STACJE ROBOCZE – 100 SZT.....	26
18.	MONITORY – 100 SZT.	31
20.	OPROGRAMOWANIE ANTYWIRUSOWE – 102 SZT.	33



1. Założenia

Celem budowy systemu teleinformatycznego jest zapewnienie dostępu do Internetu dla 60 gospodarstw domowych oraz 10 obiektów – jednostek organizacyjnych podległych gminie. Zastosowana technologia to sieć światłowodowa oraz szerokopasmowa sieć bezprzewodowa działająca w paśmie częstotliwości licencjonowanych, w systemie punkt - wielopunkt.

Jako uzupełnienie sieci w technologii wiodącej dopuszcza się zastosowanie następujących technologii:

- technologia satelitarnego dostępu do szerokopasmowego Internetu – w lokalizacjach gdzie jest to ekonomicznie lub technologicznie konieczne lub uzasadnione;
- technologia bezprzewodowa typu punkt – punkt (radiolinia) tam gdzie jest to technologicznie uzasadnione – w szczególności dla celów zapewnienia łączności pomiędzy stacjami bazowymi.

2. Wymagania

Przedmiotem opracowania jest budowa sieci szerokopasmowej zapewniającej dostęp do Internetu dla osób i jednostek zagrożonych wykluczeniem cyfrowym, w tym sieci radiowej szerokopasmowego dostępu do Internetu. Wybudowanie projektowanej sieci umożliwi dotarcie do grupy tzw. beneficjentów ostatecznych oraz na tzw. działania koordynacyjne polegające na wyposażeniu placówek edukacyjno – oświatowych w dostęp do Internetu wraz z komputerami. System ten ma być systemem dedykowanym dla grupy docelowej.

W skład sieci radiowej mają wchodzić:

- system bazowy rozumiany jako punkt zbierający sygnał transmisyjny z poszczególnych systemów wyniesionych (stacje bazowe),
- system wyniesiony rozumiany jako pojedynczy punkt dostępowy ,
- pod-system bazujący na radiowym paśmie nie-licencjonowanym, który zostanie zainstalowany dla kolejnych lokalizacji, które nie posiadają bezpośredniej widoczności ze stacją bazową lub są zainstalowane w zbyt dużej odległości od stacji bazowej.



Sieć radiowa szerokopasmowego dostępu do Internetu ma zapewnić łączność teleinformatyczną pomiędzy rozproszonymi geograficznie prywatnymi użytkownikami sieci. W tym celu konieczna jest instalacja stacji bazowej obejmującej profesjonalne systemy nadawczo-odbiorcze pracujące w licencjonowanym paśmie, systemu zarządzania siecią i usługami oraz wyposażenie wszystkich lokalizacji abonenckich w zaawansowane technologicznie urządzenia informatyczne, w tym terminale abonenckie.

Sieć światłowodowa ma zapewnić łączność pomiędzy instytucjami użyteczności publicznej (przychodnie, ośrodki kultury i oświaty) oraz stacjami bazowymi sieci radiowej. Instytucje te wyposażone zostaną w urządzenia informatyczne w tym przełączniki sieciowe, systemy podtrzymaniu pracy przy braku zasilania.

W lokalizacjach objętych projektem, w których instalacja stacji abonenckich nie jest technicznie możliwa lub nieopłacalna możliwe jest instalowanie dostępu do szerokopasmowego Internetu w technologii satelitarnej VSAT. Instalowane urządzenia muszą zapewnić usługę satelitarną dwukierunkową, co oznacza, iż zarówno odbiór, jak i przesył danych odbywa się za pośrednictwem satelity. Wymagana transmisja danych wynosi: do odbiorcy min. 2,0 Mbps, od odbiorcy min. 500 Kbps.

Powstała sieć musi mieć zapewnione łącze do krajowej sieci Internetowej, operatora krajowego. Wymagane jest techniczne zapewnienie łącza o przepustowości min 10 Mbps.

Zgodnie z wymaganiami przedstawionymi przez Gminę Besko projektowany system będzie obejmował swoim zasięgiem:

- Sieć światłowodowa - 10 następujących lokalizacji:

1. Świetlica młodzieżowa Poręby – ul. Wiejska 15, 38-524 Besko
2. Dom kultury – ul. Starowiejska 647, 38-524 Besko
3. ZS w Besku – ul. Kolejowa 54, 38-524 Besko
4. Świetlica młodzieżowa w Besku – ul. Kolejowa 56, 38-524 Besko
5. Dom Ludowy w Besku – ul. Kolejowa 56, 38-524 Besko
6. Świetlica młodzieżowa Mymoń – ul. Olza 8, 38-524 Besko
7. Zakład Gospodarki Komunalnej – ul. Starowiejska 99
8. Szkoła Podstawowa w Mymoni – ul. Szkolna
9. Gminny Ośrodek Zdrowia – ul. Błonie
10. Zespół Obiektów Sportowych w Besku – ul. Kolejowa

- Sieć bezprzewodowa (WiMAX) – 60 lokalizacji (gospodarstw domowych)



Wszystkie punkty znajdują na terenie Gminy Besko.

3. Centrum sieci

Centrum sieci (serwerownia) znajdować się będzie w budynku Gminy Besko. Serwerownia wyposażona jest w klimatyzację i system podtrzymania pracy przy braku zasilania. Serwerownię należy wyposażyć w Szafę serwerową 42U - MM 800X1000x2057H. W szafie zamontowane będą:

- Panele światłowodowe 19"/1U, 24xSC-Duplex 9/125 – 4 sztuki
- Serwery (opisane w punkcie 15)
- Przełączniki szkieletowe (opisane w punkcie 12)
- Urządzenie zabezpieczające typu Firewall (opisane w punkcie 14)

4. Łącze internetowe

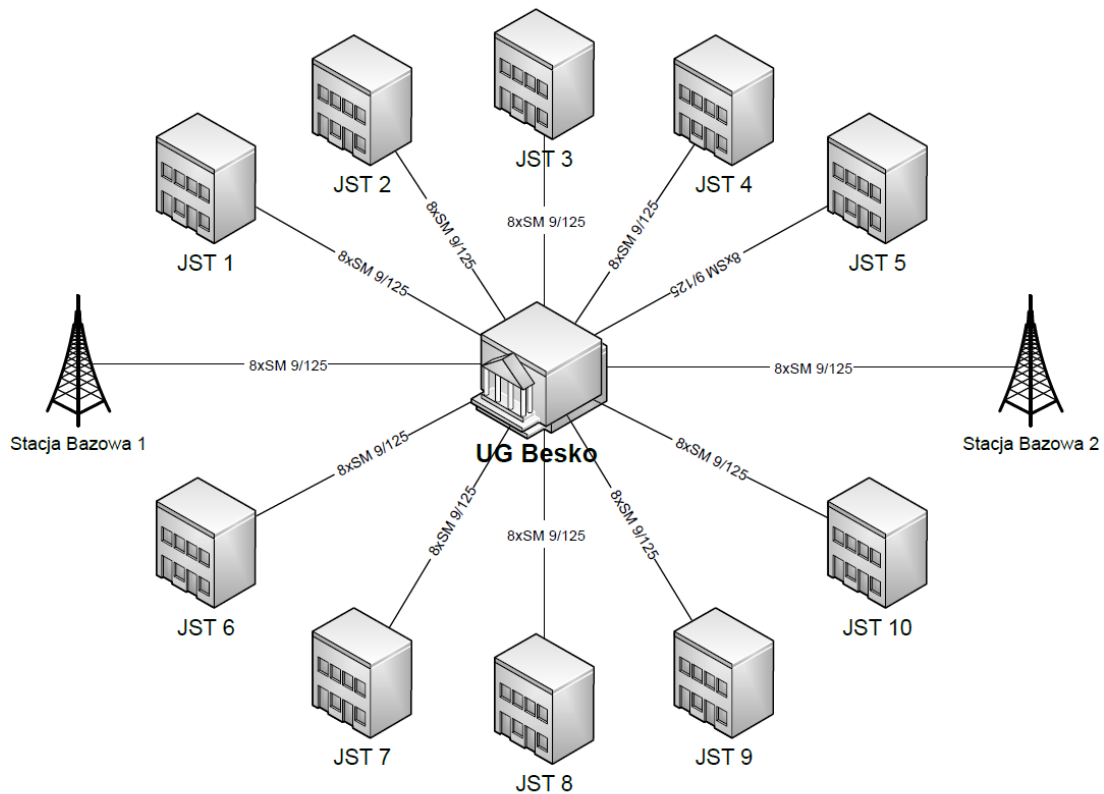
Punkt styku operatorskiego powinien zapewnić łącze do krajowej sieci Internetowej o przepustowości co najmniej 10 Mbps. W przypadku braku bezpośredniego styku należy wybudować odpowiednie łącze w optymalnej technologii. Punkt styku musi być wykonany do krajowego operatora telekomunikacyjnego. Punkt styku należy przewidzieć w budynku Urzędu Gminy, ul. Podkarpacka 5, 38-524 Besko (serwerownia).

5. Sieć światłowodowa

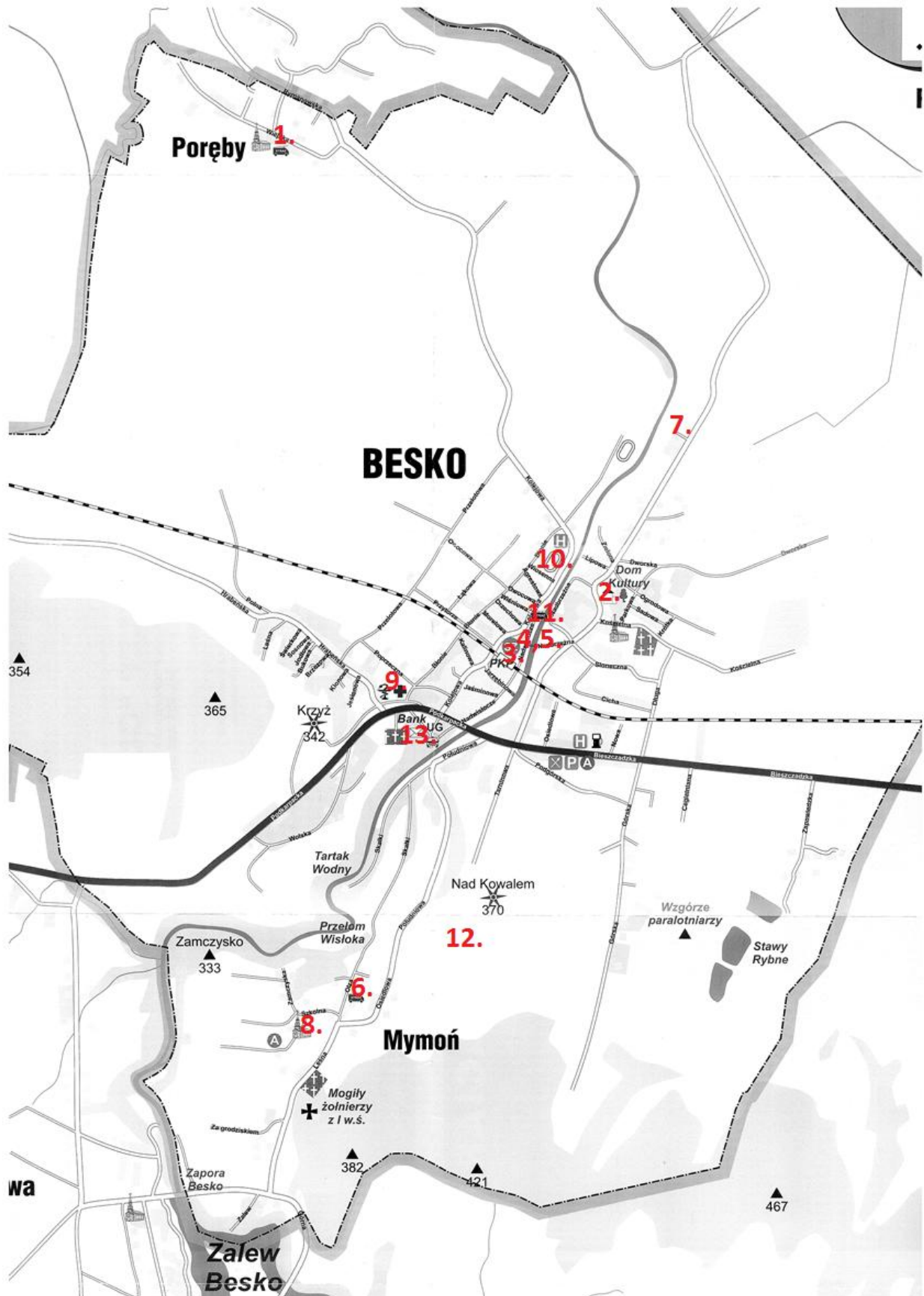
Wybudowana sieć światłowodowa ma połączyć jednostki edukacyjno – oświatowe podległe gminie (budowa kanalizacji wraz z ułożeniem kabla – minimalna długość 11 km). Budowana sieć musi być oparta na strukturze gwiazdy, czyli do każdej z łączonych lokalizacji dochodzi oddzielny kabel światłowodowy. Kable te będą zakończone w szafie serwerowej (serwerownia w budynku Gminy Besko). Po obu stronach kable muszą być zakończone w panelach światłowodowych. Aby zachować jednorodność włókien i nie powodować wprowadzania dodatkowych tłumień do toru transmisyjnego, wszystkie włókna światłowodowe należy zakończyć bezpośrednio złączami SC duplex metodą spawania.

Należy zastosować kabel światłowodowy zewnętrzny min 8 włóknowy, jednomodowy (9/125). Kabel należy ułożyć w ziemi w optotelekomunikacyjnej rurze osłonowej HDPE

wielkości min 32. Podczas przejść przez drogi asfaltowe stosować przewierty nie naruszające pasa drogowego. Kabel powinien mieć zapas min 30m w punktach początkowych i końcowych odcinka oraz co 500m w studziście teletechnicznej.



Rys 2. Schemat ideowy sieci światłowodowej



Rys. 3. Punkty do połączenia siecią światłowodową



Legenda:

1. Świetlica młodzieżowa Poręby – ul. Wiejska 15, 38-524 Besko
2. Dom kultury – ul. Starowiejska 647, 38-524 Besko
3. ZS w Besku – ul. Kolejowa 54, 38-524 Besko
4. Świetlica młodzieżowa w Besku – ul. Kolejowa 56, 38-524 Besko
5. Dom Ludowy w Besku – ul. Kolejowa 56, 38-524 Besko
6. Świetlica młodzieżowa Mymoń – ul. Olza 8, 38-524 Besko
7. Zakład Gospodarki Komunalnej – ul. Starowiejska 99
8. Szkoła Podstawowa w Mymoni – ul. Szkolna
9. Gminny Ośrodek Zdrowia – ul. Błonie
10. Zespół Obiektów Sportowych w Besku – ul. Kolejowa
11. Stacja bazowa 1
12. Stacja bazowa 2
13. Urząd Gminy w Besku – ul. Podkarpacka 5

6. Opis punktów dystrybucyjnych sieci światłowodowej

Punkty dystrybucyjne sieci światłowodowej w jednostkach JST (oznaczone numerami od 1 – 10 na Rys. 3) należy wyposażyć w :

- Szafę wiszącą 10U o wymiarach 600X420X520H
- Panel światłowodowy 19”/1U niewysuwany wyposażony 8xSC (4xDuplex) 9/125
- Dystrybucyjny przełącznik sieciowy (opisany w punkcie 13)
- Zasilacz awaryjny UPS (opisany w punkcie 16)

Punkty dystrybucyjne sieci światłowodowej przy stacji bazowej 1 (oznaczony numerem od 11 na Rys. 3) należy wyposażyć w :

- Szafę 24U stojącą - MM 600X800X1099H
- Panel światłowodowy 19”/1U niewysuwany wyposażony 8xSC (4xDuplex) 9/125
- Dystrybucyjny przełącznik sieciowy (opisany w punkcie 13)
- Zasilacz awaryjny UPS (opisany w punkcie 16)

Punkt dystrybucyjny sieci światłowodowej przy stacji bazowej 2 (oznaczony numerem 12 na Rys. 3) należy wyposażyć w :

- Szafę zewnętrzną 19 calową, stojącą z klimatyzatorem min. 18U
- Panel światłowodowy 19”/1U niewysuwany wyposażony 8xSC (4xDuplex) 9/125
- Dystrybucyjny przełącznik sieciowy (opisany w punkcie 13)



- Zasilacz awaryjny UPS (opisany w punkcie 16)

7. Lokalizacja stacji bazowych

Stacja bazowa nr 1 będzie usytuowana będzie na budynku Straży Pożarnej w Besku, stacja bazowa nr 2 na maszcie GSM w Mymoniu. Anteny tam zamontowane obejmą swoim zasięgiem cały pożądany teren.

8. Ilość sektorów, podział lokalizacji pomiędzy sektory

Ze względu na lokalizację punktów odbiorczych względem stacji nadawczych należy zastosować na każdej ze stacji bazowych 4 sektory 90 stopniowe. Stacja bazowa nr 1 będzie składać się z dwóch sektorów 90 stopni w technologii MIMO (duże zagęszczenie odbiorców) oraz dwóch sektorów 90 stopni w technologii SISO. Stacja bazowa nr 2 będzie składać się z czterech sektorów 90 stopni w technologii SISO.

9. Stacja Bazowa – 5 szt.

Minimalne wymagania dla Stacji Bazowych:

1. System ma być w pełni zgodny ze standardem 802.16e-2005 i pracować w paśmie częstotliwości 3.6-3.8GHz.
2. System ma posiadać architekturę zgodną ze standardem 802.16e-2005 tak jak to określono w sieciowym modelu odniesienia (*ang.: Network Reference Model – NRM*) poniżej.
3. Elementy systemu zdefiniowane przez blok funkcjonalny ASN (*ang.: Access Service Network*) muszą być skonstruowane w sposób umożliwiający poprawną pracę według profili A, B lub C, zgodnie z architekturą sieci określoną przez organizację WiMAX Forum
4. Stacja bazowa systemu musi posiadać kompaktową obudowę przystosowaną do instalacji zewnętrznych (tzw. rozwiązanie „All Outdoor” gdzie brak jest urządzeń aktywnych instalowanych wewnątrz pomieszczeń) zawierającą w pojedynczej obudowie kompletną część radiową, modemową, procesor/kontroler, ASN-GW oraz antenę sektorową. Stacja bazowa musi posiadać również odpowiednie złącza do podłączenie dwóch zewnętrznych anten sektorowych, zewnętrznego ASN-GW oraz systemu GPS.



5. System ma pracować poprawnie zarówno przy zachowaniu widoczności optycznej pomiędzy stacją bazową a terminalem abonenckim (*ang.: LOS*) jak również bez takiej widoczności (*ang.: NLOS*) lub ograniczonej (*ang.: nLOS*).
6. System ma poprawnie obsługiwać w tym samym czasie co najmniej takie usługi jak głos, wideo, dostęp do Internetu.
7. System powinien obsługiwać użytkowników mobilnych (tak jak definiuje to standard 802.16e), nomadycznych oraz zapewniać łącza stałe.
8. System ma obsługiwać technologię SOFDMA.
9. System ma obsługiwać kanały radiowe od 5MHz z 512 punktami FFT do 10MHz z 1024 punktami FFT bez konieczności wymiany sprzętu lub dokonywania uaktualnienia oprogramowania.
10. System ma obsługiwać technikę "Forward Error Correction" (FEC).
11. System ma obsługiwać technikę „Turbo Coding” 1/2, 2/3, 3/4 oraz 5/6.
12. System musi obsługiwać modulacje QPSK, QAM16, QAM64 z wykorzystaniem techniki korekcji błędów „Cyclic Turbo Code” zapewniając modulację QAM64 5/6 zarówno dla kierunku transmisji w stronę sieci (*ang: downlink*) jak i w stronę abonenta (*ang.: uplink*).
13. System musi obsługiwać zaawansowane techniki antenowe MIMO Tx drugiego rzędu (2 Tx) pracujące zarówno w trybie MIMO A jak również MIMO B z funkcją automatycznego przełączania pomiędzy trybami
14. System musi obsługiwać technologię "Rx diversity" (MRRC) drugiego rzędu (2 Rx) dla kierunku transmisji w stronę abonenta (*ang.: uplink*)
15. System musi zapewniać zwiększoną odporność na zakłócenia poprzez wielokrotne rozgłaszanie opisu dostępu w pojedynczej ramce (MAP).
16. System musi obsługiwać technikę HARQ.
17. System musi posiadać wbudowany analizator widma
18. System musi obsługiwać technikę automatycznej kontroli mocy transmisyjnej (*ang.: Automatic transmit power control - ATPC*).
19. Zmiany modulacji w systemie (QPSK, QAM16, QAM64) muszą następować automatycznie w sposób dynamiczny.
20. Pojedyncza stacja bazowa systemu (pojedyncza obudowa) musi zapewnić obsługę dwóch niezależnych sektorów (konfiguracja: 1 stacja bazowa + 2 sektory), każdy pracujący opcjonalnie na kanale 7MHz (2 x 7MHz) oraz 10MHz (2 x 10MHz).
21. System musi pracować w technologii TDD (*ang.: Time Division Duplex*) wykorzystując co najmniej następujące szerokości kanałów: 5MHz, 7MHz, 10MHz, 2x7MHz oraz 2x10MHz
22. Moc transmisyjna nadajnika radiowego mierzona na porcie RF anteny nie może być mniejsza niż 30 dBm.
23. System musi być zasilany ze źródła napięcia stałego -48Vdc.
24. System musi obsługiwać jednocześnie technikę ETH-CS oraz IP-CS



25. System musi posiadać wbudowany serwer DHCP i obsługiwać opcję 82 oraz DHCP opcja trybu transparentnego
26. System musi obsługiwać mechanizmy klasyfikacji ruchu w oparciu o DSCP, PPPoE, VLAN priority lub VLAN ID
27. System musi obsługiwać mechanizm 802.1Q tagging.
28. System musi posiadać elastyczną architekturę umożliwiającą lokalne lub centralne (przez serwer AAA) kreowanie usług jednocześnie pracując w trybie centralnego lub rozproszonego (wbudowanego w systemie) ASN-GW.
29. Mechanizm autentykacji w systemie musi odbywać się za pomocą protokołu RADIUS poprzez EAP-TTLS
30. System musi obsługiwać algorytmy kodowania AES 128bit. Klucze AES muszą być generowane w sposób dynamiczny przy każdorazowym logowaniu się użytkownika w sieci.
31. System musi posiadać mechanizmy “uczenia się” adresów MAC w celu zapewnienia optymalizacji ruchu (zapobieganie przepelnieniu).
32. Stacja bazowa systemu musi być wyposażona w interfejs Ethernet 100/10 MB/s w celu podłączenia stacji do sieci transmisyjnej (szkieletowej).
33. System musi umożliwiać wykorzystanie tylko jednego odbiornika GPS do synchronizacji co najmniej 4 stacji bazowych zainstalowanych w jednej lokalizacji.
34. Stacja Bazowa musi mieć możliwość zasilania elektrycznego zgodnego ze standardem PoE (*ang.: Power over Ethernet*), Jednostki Abonenckiej służącej jako dostęp do sieci szkieletowej za pomocą wbudowanego w Stację Bazową interfejsu sieciowego.
35. Obudowa systemu musi posiadać Współczynnik Ochrony IP65 i IP67

Gwarancja: min. 2 lata gwarancji producenta

10. Terminale abonenckie – 60 szt.

Minimalne wymagania dla terminali abonenckich:

1. Terminal abonencki musi być w pełni zgodny ze standardem 802.16e-2005
2. Terminal abonencki musi zapewnić prawidłowe działanie ze stacją bazową systemu na podstawie testów certyfikacyjnych 802.16e-2005 wave 2 określonych przez organizację WiMAX Forum
3. Terminal abonencki musi pracować w paśmie częstotliwości 3.6-3.8GHz oraz zapewnić prawidłowe działanie ze stacją bazową systemu oraz przy zastosowaniu testów certyfikacyjnych 802.16e-2005 wave 2 określonych przez organizację WiMAX Forum
4. Terminal abonencki musi obsługiwać skalowalną technologię OFDMA 512/1024 FFT (*ang.: scalable OFDMA*)
5. Terminal abonencki musi pracować w technologii TDD (*ang.: Time Division Duplex*)
6. Terminal abonencki musi obsługiwać modulacje QPSK, QAM16 oraz QAM64.
7. Terminal abonencki musi obsługiwać zaawansowane techniki antenowe MIMO pracujące zarówno w trybie MIMO A jak również MIMO B oraz technikę MRC (*ang.: Maximum Ratio Combining*)



8. Terminal abonencki musi posiadać dwie opcje konfiguracyjne: opcja z anteną zintegrowaną (część zewnętrzna radiowa jest zintegrowana z anteną w sposób kompaktowy) oraz opcja z anteną oddzielną (wymagany jest interfejs RF w części radiowej do podłączenia odrębnej anteny)
9. Maksymalna moc transmisyjna terminala abonenckiego mierzona na porcie radiowym RF anteny nie może być niższa niż 21 dBm.
10. Terminal abonencki powinien zapewniać możliwość klasyfikacji ruchu oraz funkcje zapewniania jakości usług (*ang.: Quality of Service – QoS*) w oparciu o mechanizm IP DSCP (*ang.: Differentiated Services Code Point*)
11. Terminal abonencki powinien obsługiwać funkcjonalność IP CS (w trybie „bridge”) z transparentnym ruchem DHCP
12. Terminal abonencki powinien obsługiwać funkcjonalność ETH CS z możliwością klasyfikacji ruchu DSCP, PPPoE, VLAN ID (802.1q), VLAN priority (802.1p)
13. Jednostka Abonencka ma wykorzystywać funkcjonalność multi-host czyli możliwość pracy z co najmniej dwoma adresami IP na porcie WAN.
14. Terminal abonencki powinien być zarządzany lokalnie lub zdalnie za pomocą zwykłej przeglądarki internetowej
15. Jednostka abonencka ma obsługiwać protokół TR-069 lub OMA-DM dla centralnego zarządzania za pomocą oprogramowania ACS
16. Terminal abonencki powinien obsługiwać algorytmy kodowania AES 128bit
17. Temperatury otoczenia w jakich terminal abonencki ma działać poprawnie muszą wynosić co najmniej: od -5C do 45C dla części wewnętrznych terminala oraz od -40C do 55C dla części zewnętrznych
18. Terminal abonencki powinien być wyposażony w interfejs Ethernet (RJ-45) z funkcją PoE (*ang.: Power over Ethernet*)

Gwarancja: min. 2 lata gwarancji producenta

11. System zarządzania siecią WiMAX – 1 szt.

Minimalne wymagania dla systemu zarządzania siecią WiMAX:

1. Automatyczne i manualne wykrywanie elementów sieci takich jak Stacje Bazowe, Jednostki Abonenckie itp. System powinien zachowywać dane wszystkich elementów systemu.
2. Zarządzanie Jednostkami Abonenckimi musi odbywać się za pomocą protokołu TR-69.
3. System powinien zapewniać łatwość obsługi, intuicyjny interfejs webowy oraz wszechstronny podręcznik użytkownika/pomoc systemu.
4. Filtry i wyszukiwanie: ma być możliwe predefiniowanie filtrów użytkownika pozwalających na przeszukiwanie takich danych jak: alarmy oraz elementy sieci.
5. Bezpieczeństwo: zaimplementowane mechanizmy kontroli i ograniczania dostępu do systemu zarządzania



6. Możliwość zdalnego wgrania oprogramowania przez radio .
7. Wszechstronne zarządzanie za pomocą protokołu SNMP.
8. Administracja Systemem
 - 8.1. Dodawanie/zmiana/konfiguracja/weryfikacja/usuwanie/zarządzanie kontem użytkownika końcowego w systemie
 - 8.2. Dodawanie/zmiana/konfiguracja/weryfikacja/usuwanie/zarządzanie elementami sieci w bazie danych.
 - 8.3. Dodawanie/zmiana/konfiguracja/weryfikacja/usuwanie/zarządzanie lokalizacjami w systemie.
 - 8.4. Musi być możliwa kontrola i ograniczanie praw, przywilejów oraz autoryzacji operatora.
 - 8.5. Kontrola dostępu ma umożliwiać klasyfikację grup operatorów ze wspólnymi charakterystycznymi prawami, z możliwością ograniczenia lub rozszerzenia praw dostępu dla pojedynczego użytkownika.
 - 8.6. Możliwość ograniczenia dostępu do elementów sieci oraz/lub do logów.
 - 8.7. Mają być dostępne logi wszystkich wiadomości pomiędzy Systemem Zarządzania I Elementami Sieci.
 - 8.8. Musi być możliwość oceny Operatora, który zainicjował wiadomość.
 - 8.9. Musi być możliwość definiowania Użytkowników z różnymi wymaganiami dot. klas usługowych. Ma być możliwość wpierania klas usługowych dla takich aplikacji jak głos czy multimedia.
9. Zarządzanie urządzeniami.
 - 9.1. Automatyczne i manualne wykrywanie elementów sieci takich jak Stacje Bazowe, Jednostki Abonenckie itp. System powinien zachowywać dane wszystkich elementów systemu.
 - 9.2. Pokazywanie podłączonych elementów sieci korzystając z bazy danych, dając kompletny widok sieci bez fizycznego sprawdzania każdego ze zdalnych urządzeń
 - 9.3. Zarządzanie alarmami: Alarmy muszą być zbierane z całej sieci, przechowywane w bazie danych i pokazywane zgodnie z użytym filtrem w widoku alarmów.
 - 9.4. Zarządzanie kontrolą jakości pracy elementów sieci.

12. Szkieletowe przełączniki sieciowe – 2 szt.

Minimalne parametry przełączników szkieletowych sieci (serwerownia w budynku Gminy Besko).



Przełącznik szkieletowy Typu A – 1 szt.

Przełącznik należy wyposażyć w 13 sztuk jednomodowych wkładek SFP. Wkładki muszą być tego samego producenta co przełącznik.

- 1) Musi być oparte o urządzenie o zamkniętej konfiguracji, wysokości 1 RU;
- 2) Urządzenie musi posiadać tzw. SwitchingFabric o wydajności co najmniej 160 Gbps oraz przepustowość co najmniej 35 Mpps;
- 3) Obsługa na poziomie minimum 255 aktywnych sieci wirtualnych (VLAN);
- 4) Urządzenie musi być przystosowane do instalacji w szafie telekomunikacyjnej rack 19”;
- 5) Urządzenie musi być wyposażone w następujące interfejsy:
 - a) 12 portów Gigabit Ethernet na moduły SFP,
 - b) Moduł pozwalający obsadzić 4 porty 1 Gigabit Ethernet w oparciu o wkładki SFP, 13 sztuk jednomodowych wkładek SFP współpracujących z oferowanym przełącznikiem
- 6) Urządzenie musi posiadać redundantne, modułowe chłodzenie;
- 7) Urządzenie musi posiadać możliwość łączenia w stos logiczny przełączników (do 9 przełączników w jednym stosie) umożliwiając komunikację z wydajnością min. 64 Gbps pomiędzy nimi. Stos przełączników musi mieć możliwość zarządzania jednym adresem IP;
- 8) Urządzenie musi posiadać możliwość łączenia w stos zasilający przełączników (do 4 przełączników w jednym stosie). Urządzenia połączone w stos zasilający mają w przypadku awarii jednego z zasilaczy umożliwiać dostarczenie zasilania z innego urządzenia ze stosu;
- 9) Urządzenie musi mieć możliwość instalacji modułów posiadających 2 porty 10GbE (X2), 2 porty 10GB-T (RJ45) lub 4 porty 1GbE (SFP lub GBIC);
- 10) Urządzenie musi posiadać sprzętowe wsparcie dla protokołu 802.1AE;
- 11) Obsługa ramek jumbo (9216Bytes);
- 12) Funkcjonalność DHCP snooping;
- 13) Mechanizmy związane z zapewnieniem ciągłości pracy sieci:
 - a) IEEE 802.1s RapidSpanningTree,
 - b) IEEE 802.1w Multi-Instance Spanning Tree;
- 14) Obsługa protokołów routingu: statyczny, RIP v2;
- 15) Możliwość grupowania portów zgodnie ze specyfikacją IEEE 802.3ad (LACP);
- 16) Mechanizmy związane z zapewnieniem jakości usług w sieci:
 - a) klasyfikacja ruchu do klas różnej jakości obsługi (QoS),
 - b) implementacja co najmniej ośmiu kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu Round Robin lub podobnego dla obsługi tych kolejek,
 - c) obsługa jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (StrictPriority),
 - d) możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP,
 - e) możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kb/s (policing, ratelimiting),
 - f) zarządzanie kolejkami za pomocą tail drop lub podobny;



- 17) Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
- a) min. 5 konfigurowalnych poziomów dostępu administracyjnego poprzez konsolę,
 - b) autoryzacja użytkowników/portów w oparciu o IEEE 802.1X z możliwością przydziału listy kontroli dostępu (ACL) i VLANu,
 - c) dostęp do urządzenia przez:
 - i. HTTPS,
 - ii. SNMPv3 (ang. Simple Network Management Protocol version 3),
 - iii. SSHv2 (także IPv6),
 - d) możliwość rozszerzenia oprogramowania do wsparcia funkcjonalności prywatnego VLAN-u, czyli możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. porty izolowane) z pozostawieniem możliwości komunikacji z portem nadrzędnym,
 - e) współpraca z systemami kontroli dostępu do sieci typu NAC, NAP lub równoważnym,
 - f) możliwość filtrowania ruchu na poziomie portu oraz VLANu w oparciu o adresy MAC, IP, porty TCP/UDP,
 - g) możliwość synchronizacji czasu zgodnie z NTP;
- 18) Możliwość tworzenia zestawów konfiguracyjnych dla portów (grupy poleceń umożliwiające konfigurację wielu funkcjonalności za pomocą jednego polecenia);
- 19) Możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu lub poprzez określony VLAN;
- 20) Zarządzanie poprzez interfejs CLI (konsolę), HTTP, SNMP;
- 21) Musi umożliwiać identyfikację i uwierzytelnianie w oparciu o serwer RADIUS;

Gwarancja: min. 2 lata gwarancji producenta sprzętu

Przełącznik szkieletowy Typu B – 1 szt.

Przełącznik należy wyposażyć w jednomodową wkładkę SFP (1 sztuka). Wkładka musi być tego samego producenta co przełącznik – nie dopuszcza się stosowania zamienników.

- Ma być oparte o urządzenie o zamkniętej konfiguracji, wysokości 1 RU.
- Urządzenie ma posiadać przynajmniej 128MB pamięci DRAM oraz 64MB pamięci Flash
- Urządzenie musi obsługiwać 8000 adresów MAC
- Urządzenie musi posiadać tzw. Switching Fabric o wydajności co najmniej 50 Gbps oraz przepustowość co najmniej 38,7 Mpps
- Urządzenie musi posiadać co najmniej 24 portów Gigabit Ethernet w standardzie 10/100/1000BaseT plus dwa porty typu uplink Small Form-Factor Pluggable (SFP) pozwalające na instalację wkładek z portami Gigabit Ethernet 1000BASE-T, 1000BASE-SX, 1000BASE-ZX, 1000BASE LX/LH.
- Urządzenie musi posiadać wsparcie dla co najmniej 64 sieci VLAN oraz 4000 VLAN ID.
- Urządzenie musi mieć wsparcie protokołów sieciowych zgodnie ze standardami:



- IEEE 802.1x
- IEEE 802.1s
- IEEE 802.1w
- IEEE 802.3x full duplex na portach 10BASE-T, 100BASE-TX oraz 1000BASE-T
- IEEE 802.3ad
- IEEE 802.1D
- IEEE 802.1p
- IEEE 802.1Q
- IEEE 802.3 10BASE-T
- IEEE 802.3u 100BASE-TX
- IEEE 802.3z 1000BASE-X
- IEEE 802.3ab 100BASE-T
- Urządzenie ma wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
 - a. Mechanizm zapewnienia jakości usług CoS
 - b. Mechanizm kolejkowania Shaped Round Robin (SSR).
- Urządzenie ma wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
 - a. Możliwość uzyskania dostępu do urządzenia przez SSHv2 i SNMPv3
 - b. Możliwość autoryzacji prób logowania do urządzenia za pomocą serwerów RADIUS.
 - c. Możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. protected ports) z pozostawieniem możliwości komunikacji z portem nadrzednym (designated port) lub funkcjonalność Private VLAN Edge
 - d. możliwość tworzenia portów monitorujących, pozwalających na kopiowanie na port monitorujący ruchu z innego dowolnie wskazanego portu lub sieci VLAN z lokalnego przełącznika
 - e. ochrona przed rekonfiguracją struktury topologii Spanning Tree spowodowana przez niepowołane i nieautoryzowane urządzenie sieciowe
 - f. min. 5 poziomów uprawnień do zarządzania urządzeniem (z możliwością konfiguracji zakresu dostępnych funkcjonalności i komend)
 - g. współpraca z systemami kontroli dostępu do sieci typu NAC, NAP itp.
- Ma wspierać obsługę ruchu multicast z wykorzystaniem IGMPv3 oraz możliwość utworzenia co najmniej 255 grup
- Urządzenie musi umożliwiać grupowanie portów w jeden kanał logiczny zgodnie z LACP
- Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line. Tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nielotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.



- Urządzenie musi mieć możliwość ochrony przed rekonfiguracją struktury topologii Spanning Tree spowodowana przez niepowołane i nieautoryzowane urządzenie sieciowe.
- Urządzenie ma być zarządzane przy pomocy bezpłatnej aplikacji graficznej dostarczonej przez producenta.
- Urządzenie musi mieć możliwość montażu w szafie 19", a jego obudowa musi być wykonana z metalu.

Gwarancja: min. 2 lata gwarancji producenta

13. Dystrybucyjne przełączniki sieciowe – 12 szt.

Minimalne parametry przełączników sieciowych zapewniających połączenie jednostek podległych gminie JST oraz stacji bazowych wskazanych w punkcie 5 z siecią szkieletową.

Każdy przełącznik należy wyposażyć w jednomodową wkładkę SFP (1 sztuka). Wkładka musi być tego samego producenta co przełącznik – nie dopuszcza się stosowania zamienników.

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



- Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
 - c. Mechanizm zapewnienia jakości usług CoS
 - d. Mechanizm kolejkowania Shaped Round Robin (SSR).
- Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
 - h. Możliwość uzyskania dostępu do urządzenia przez SSHv2 i SNMPv3
 - i. Możliwość autoryzacji prób logowania do urządzenia za pomocą serwerów RADIUS.
 - j. Możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. protected ports) z pozostawieniem możliwości komunikacji z portem nadrzednym (designated port) lub funkcjonalność Private VLAN Edge
 - k. możliwość tworzenia portów monitorujących, pozwalających na kopiowanie na port monitorujący ruchu z innego dowolnie wskazanego portu lub sieci VLAN z lokalnego przełącznika
 - l. ochrona przed rekonfiguracją struktury topologii Spanning Tree spowodowana przez niepowołane i nieautoryzowane urządzenie sieciowe
 - m. min. 5 poziomów uprawnień do zarządzania urządzeniem (z możliwością konfiguracji zakresu dostępnych funkcjonalności i komend)
 - n. współpraca z systemami kontroli dostępu do sieci typu NAC, NAP itp.
- Musi wspierać obsługę ruchu multicast z wykorzystaniem IGMPv3 oraz możliwość utworzenia co najmniej 255 grup
- Urządzenie ma umożliwiać grupowanie portów w jeden kanał logiczny zgodnie z LACP
- Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line. Tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej ma być możliwe uruchomienie urządzenia z nową konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.
- Urządzenie musi mieć możliwość ochrony przed rekonfiguracją struktury topologii Spanning Tree spowodowana przez niepowołane i nieautoryzowane urządzenie sieciowe.
- Urządzenie musi być zarządzane przy pomocy bezpłatnej aplikacji graficznej dostarczonej przez producenta.
- Urządzenie ma mieć możliwość montażu w szafie 19", a jego obudowa ma być wykonana z metalu.

Gwarancja: min. 2 lat gwarancji producenta

14. Urządzenie zabezpieczające typu Firewall – 1 szt.



Minimalne parametry zapory sieciowej typu Firewall znajdującej się na styku z siecią operatora zapewniającego dostęp do sieci Internet.

1. Urządzenie powinno pełnić rolę ściany ogniowej śledzącej stan połączeń z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji
2. Powinno być oparte o dedykowany system operacyjny – nie dopuszcza się rozwiązań gdzie platformą systemową jest otwarty system operacyjny np. UNIX (Linux, FreeBSD etc.) lub jego modyfikacja
3. Urządzenie nie powinno posiadać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej
4. Urządzenie musi posiadać co najmniej cztery porty 10/100 FastEthernet oraz jeden port 10/100 FastEthernet dla zarządzania OOB (Out of Band)
5. Powinno posiadać dedykowane dwa porty dla podłączenia konsoli oraz dla uzyskania zdalnego dostępu przez modem asynchroniczny
6. Powinno posiadać co najmniej jeden port USB dla przyszłych zastosowań (tokeny, etc.)
7. Powinno posiadać co najmniej 256MB DRAM oraz 64MB Flash
8. Urządzenie powinno posiadać dodatkowy slot pozwalający na wykorzystanie modułów funkcjonalnych zwiększających standardowe możliwości urządzenia, w szczególności:
 - a. moduł umożliwiający osiągnięcie pełnej funkcjonalności systemu IPS (Intrusion Prevention System)
 - b. moduł umożliwiający osiągnięcie funkcjonalności ochrony antywirusowej, antyspyware, antyspamowej, filtrowania i blokowania odwołań do niepożądanych adresów URL oraz filtrowania zawartości poczty elektronicznej e-mail
 - c. uzyskanie co najmniej czterech dodatkowych portów 10/100/1000 GigabitEthernet
9. Oczekiwane jest, że w dostarczonym urządzeniu zaimplementowana będzie pełna funkcjonalność ochrony antywirusowej i antyspyware. Wymaga się, aby moduł obsługiwał dla tej funkcjonalności minimum 150 użytkowników – możliwość większej liczby po zastosowaniu dodatkowej licencji.
10. Urządzenie musi posiadać zintegrowane sprzętowe wsparcie dla szyfrowania
11. Urządzenie powinno mieć możliwość operowania jako transparentna ściana ogniowa warstwy drugiej ISO OSI
12. Urządzenie powinno umożliwiać terminowanie co najmniej 250 jednoczesnych sesji VPN opartych o protokół IPSEC
13. Na urządzeniu powinna istnieć możliwość terminowania jednocześnie 2 sesji WebVPN z możliwością rozbudowy do 250 sesji po zastosowaniu dodatkowej licencji.
14. Urządzenie powinno obsługiwać co najmniej 50 000 jednoczesnych sesji/połączeń z prędkością 9000 połączeń na sekundę
15. Przepustowość obsługiwana przez urządzenie nie powinna być mniejsza niż 300 Mbps i jednocześnie 170 Mbps dla ruchu szyfrowanego symetrycznymi algorytmami 3DES/AES
16. Wraz z urządzeniem powinno być dostarczane oprogramowanie klienta VPN, umożliwiające instalację go i zestawienie do urządzenia połączeń VPN z komputerów osobistych PC pracujących pod kontrolą systemów operacyjnych Windows, Solaris i



- Linux, a także komputerów Mac. Oprogramowanie to powinno pochodzić od tego samego producenta, co oferowane urządzenie i powinno być objęte jego jednolitym wsparciem technicznym.
17. Urządzenie powinno umożliwiać obsługę co najmniej 50 interfejsów VLAN w standardzie 802.1q.
 18. Urządzenie powinno w celu redundancji umożliwiać implementację funkcji niezawodności pary takich urządzeń, czyli tzw. failover działającego w trybie active/standby lub active/active po zastosowaniu dodatkowej licencji.
 19. Urządzenie powinno umożliwiać obsługę minimum 5 wirtualnych instancji firewall po zastosowaniu dodatkowej licencji.
 20. Powinno dokonywać inspekcji ruchu voice w zakresie protokołów H.323, SIP, SCCP, MGCP, TAPI, JTAPI
 21. Urządzenie powinno mieć możliwość blokowania aplikacji typu „internetowy komunikator” wykorzystujących port 80 (np.: Skype, MSN)
 22. Urządzenie powinno mieć możliwość blokowania aplikacji typu peer-to-peer (np: Kaaza, eDonkoey)
 23. Urządzenie powinno mieć możliwość inspekcji protokołów HTTP oraz FTP na nie standardowych portach
 24. Urządzenie powinno zapewniać wsparcie dla list kontroli dostępu dla IPv6
 25. Urządzenie powinno być zarządzalne przy wykorzystaniu dedykowanej aplikacji umożliwiającej płynną (z użyciem kreatorów) konfigurację poszczególnych funkcji urządzenia.
 26. Urządzenie powinno być przystosowane do montażu w 19-in szafie rackowej i nie zajmować więcej miejsca niż 1RU (rack unit)

Gwarancja: min. 2 lata gwarancji producenta

15. Minimalne parametry techniczne serwera – 2 szt.

Parametr	Charakterystyka (wymagania minimalne)
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 dwuprocessorowych
Procesor	Jeden procesor czterordzeniowy klasy x86 dedykowany do pracy w serwerach zaprojektowany do pracy w układach dwuprocessorowych, taktowany zegarem co najmniej 2.4GHz, pamięć cache L3 12 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	8 GB DDR3 1333 MHz RDIMM, płyta główna musi obsługiwać minimum 64GB, na płycie głównej ma znajdować się minimum 8 slotów przeznaczonych dla pamięci, możliwość instalacji kości pamięci RDIMM lub UDIMM.
Zabezpieczenia pamięci RAM	ECC, SBEC, SDDC (lub równoważny), Memory Mirror.
Gniazda PCI	Minimum 3 złącza PCI-E drugiej generacji
Interfejsy sieciowe	Minimum 2 porty typu 10/100/1000 wbudowane na płycie głównej.
Interfejs urządzeń zewnętrznych	Minimum 2 portowy kontroler urządzeń zewnętrznych SAS 2.0
Napęd optyczny	Wewnętrzny napęd DVD+/-RW
Dyski twarde	Możliwość instalacji min. 8 dysków SATA, SAS oraz SSD. Zainstalowane 2 dyski 300GB typu HotPlug SAS 15krpm.
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, 2 x RJ-45, VGA, 1 port szeregowy
Video	Zintegrowana karta graficzna, umożliwiająca rozdzielczość min. 1280x1024.
Zasilacze	Wysokowydajne, redundatne zasilacze o mocy maksymalnie 750W.
Bezpieczeństwo	Zintegrowany z płytą główną moduł TPM, możliwość zainstalowania wewnętrznej karty pamięci SD oraz klucza USB.
Diagnostyka	Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o adresie IP, stanie procesora, pamięci, dysków, aktualnym poborze mocy oraz wysokości temperatury.
Karta Zarządzania	Zintegrowana z płytą główną lub zainstalowana w dedykowanym slotcie karta zarządzająca niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane złącze RJ-45 i umożliwiająca: zdalny dostęp do graficznego interfejsu Web karty zarządzającej <ul style="list-style-type: none"> ▪ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera,) ▪ 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 Management); SNMP; IPMI2.0, VLAN tagging, Telnet, SSH ▪ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer ▪ możliwość zdalnego ustawienia limitu poboru prądu przez

	<p>konkretny serwer</p> <ul style="list-style-type: none">▪ 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
Zarządzanie	<p>Zintegrowany z płytą główną moduł zawierający sterowniki do systemów operacyjnych i oprogramowanie zgodne ze standardem UEFI umożliwiające:</p> <ul style="list-style-type: none">▪ uaktualnienie przechowywanych sterowników i firmware'u urządzeń▪ konfigurację kontrolera RAID▪ instalację systemu operacyjnego bez konieczności korzystania z dodatkowej płyty ze sterownikami
System Operacyjny	<p>Serwerowy system operacyjny musi posiadać następujące cechy.</p> <ol style="list-style-type: none">1. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych,2. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,3. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play),4. Graficzny interfejs użytkownika,5. Obsługa systemów wieloprocessorowych,6. Obsługa platform sprzętowych x86, x64,7. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu,8. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania):<ol style="list-style-type: none">a. Podstawowe usługi sieciowe: DNS, DHCPb. Usługi katalogowe pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe)c. Zdalna dystrybucja oprogramowania na stacje roboczed. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczeje. PKI (Centrum Certyfikatów, obsługa klucza publicznego i prywatnego)



	<p>f. Szyfrowanie plików i folderów</p> <p>g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec)</p> <p>h. Możliwość rozłożenia obciążenia serwerów</p> <p>i. Serwis udostępniania stron WWW</p> <p>j. Serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management)</p> <p>k. Wsparcie dla protokołu IP w wersji 6 (IPv6)</p> <p>9. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.</p>
Certyfikaty	<p>Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001.</p> <p>Deklaracja CE.</p> <p>Wymagane jest dostarczenie odpowiednich certyfikatów.</p>
Warunki gwarancji	<p>Przynajmniej 5 lat gwarancji z czasem reakcji w następnym dniu roboczym, przyjmowanie zgłoszeń 24 godziny na dobę, 7 dni w tygodniu.</p> <p>W przypadku awarii dysku twardego, uszkodzony dysk pozostaje u Zamawiającego.</p> <p>Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta serwera – dokumenty potwierdzające załączyć do oferty.</p> <p>Oświadczenie producenta serwera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.</p>
Dokumentacja użytkownika	<p>Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</p> <p>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p>

16. Zasilacz awaryjny UPS – 12 szt.

Minimalne wymagania dla UPS Typ A (2 sztuki):

Parametr	Wymagania minimalne
Moc pozorna	3000 VA
Moc rzeczywista	2700 Wat



Architektura UPSa	on-line
Maks. czas przełączenia na baterię	0 ms
Liczba i rodzaj gniazdek z utrzymaniem zasilania	<ul style="list-style-type: none"> • 8 x IEC320 C13 (10A) • 1 x IEC320 C19 (16A)
Liczba, typ gniazd wyj. z ochroną antyprzepięciową	1 x IEC320 C19 (16A)
Typ gniazda wejściowego	IEC320 C20 (16A)
Czas podtrzymania dla obciążenia 100%	3 min
Czas podtrzymania przy obciążeniu 50%	9 min
Zakres napięcia wejściowego w trybie podstawowym	160-276 V
Zimny start	Tak
Układ automatycznej regulacji napięcia (AVR)	Tak
Sinus podczas pracy na baterii	Tak
Porty komunikacji	<ul style="list-style-type: none"> • RS232 (DB9) • USB
Diody sygnalizacyjne	<ul style="list-style-type: none"> • autotest • konieczna wymiana baterii • praca z baterii • praca z sieci zasilającej • pracy w trybie bypass • przeciążenia UPSa • stan obciążenia UPSa
Alarmy dźwiękowe	<ul style="list-style-type: none"> • awaria • praca w trybie bypass • praca z baterii • znaczne wyczerpanie baterii
Typ obudowy	rack 19"
Wyposażenie standardowe	<ul style="list-style-type: none"> • DB-Slot - gniazdo na dodatkowe karty komunikacyjne - 1szt. • kabel komunikacyjny • kabel zasilający 1.8m IEC320 C13/C14
Dodatkowe funkcje	<ul style="list-style-type: none"> • system ładowania nieciągniętego baterii ABM przedłuża żywotność akumulator o 50%



	<ul style="list-style-type: none"> wydłużenie czasu podtrzymania poprzez dołożenie dodatkowych zewnętrznych baterii
Znaki bezpieczeństwa	CE, GS
Standardy	EN-62040-1, IEC 60950-1
EMC	EN-62040-2:2006; Emisja – kat. C1, Odporność – kat. C2
Gwarancja	Min. 3 lata gwarancji producenta

Minimalne wymagania dla UPS Typ B (10 sztuk):

Parametr	Wymagania minimalne
Moc pozorna	500 VA
Moc rzeczywista	300 Wat
Architektura UPSa	line-interactive
Maks. czas przełączenia na baterię	1,5 ms
Liczba i rodzaj gniazdek z utrzymaniem zasilania	2 x PL (10A)
Liczba, typ gniazd wyj. z ochroną antyprzepięciową	2 x PL (10A)
Typ gniazda wejściowego	kabel z wtykiem PL (10A)
Czas podtrzymania dla obciążenia 100%	1,5 min
Czas podtrzymania przy obciążeniu 50%	5 min
Zakres napięcia wejściowego w trybie podstawowym	180-264 V
Zmienny zakres napięcia wejściowego	177-267 V
Zimny start	Tak
Układ automatycznej regulacji napięcia (AVR)	Nie
Sinus podczas pracy na baterii	Tak
Porty komunikacji	RS232 (DB9)
Port zabezpieczający linie danych	RJ11 - linia modemowa/faxowa, DSL
Diody sygnalizacyjne	<ul style="list-style-type: none"> praca z sieci zasilającej praca z baterii przeciążenia UPSa
Alarmy dźwiękowe	<ul style="list-style-type: none"> awaria znaczne wyczerpanie baterii przeciążenie UPSa



Typ obudowy	rack 19"
Wyposażenie standardowe	kabel komunikacyjny
Dodatkowe funkcje	przełączniki konfiguracyjne
Dołączone oprogramowanie	<ul style="list-style-type: none"> • Dla Novell NetWare 4.x, 5.x, 6 • Dla Win95/98/NT/2000/2003/XP, Linux, FreeBSD • Dla HP-UX/IBM AIX/Mac OS/Linux/Unix

17. Stacje Robocze – 100 szt.

Minimalne parametry techniczne stacji roboczych dla gospodarstw domowych (60 sztuk) oraz jednostek podległych JST (40 sztuk).

Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
Procesor	Procesor osiągający w wynikach testów wyniki: Sysmark 2007 Overall – min. 215 pkt., Sysmark 2007 Productivity – min. 221 pkt., Sysmark 2007 3D – min. 233 pkt. (wyniki dostępne na stronie http://www.anandtech.com)
Pamięć operacyjna	4GB, możliwość rozbudowy do min 16GB
Parametry pamięci masowej	Min. 250 GB. Dysk twarde o pojemności przynajmniej 250GB. Powinna istnieć możliwość podłączenia drugiego wewnętrznego dysku twardego.
Grafika	Grafika zintegrowana z procesorem powinna umożliwiać pracę dwumonitorową ze wsparciem dla HDMI v1.4 z 3D, ze sprzętowym wsparciem dla kodowania H.264 oraz MPEG2, DirectX 10.1, OpenGL 3.0, Shader 4.1 posiadająca min. 6EU (Graphics Execution Units) oraz Dual HD HW Decode o max rozdzielczości 2560x1600 @ 60Hz (cyfrowo) i 2048x1536 @ 75Hz (analogowo)
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik 2W w obudowie komputera Porty słuchawek i mikrofonu na przednim oraz na tylnym panelu obudowy.
Obudowa	Typu „MiniTower” z obsługą kart PCI 32bit oraz PCI Express wyłącznie o pełnym profilu, wyposażona w min. 4 kieszenie: 2 szt 5,25” zewnętrzne i 2 szt 3,5” wewnętrzne Zasilacz o mocy max 265W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 90%,
Zgodność z systemami operacyjnymi i standardami	Oferowane modele komputerów muszą posiadać certyfikat, potwierdzający poprawną współpracę oferowanych modeli komputerów z oferowanym systemem operacyjnym w wersji 32bit i 64bit (załączyć wydruk ze strony WHCL).



<p>Certyfikaty standardy i</p>	<ul style="list-style-type: none"> – Certyfikat ISO9001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu) – Deklaracja zgodności CE (załączyć do oferty) – Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia 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 – Komputer musi spełniać wymogi normy Energy Star 5.0 Wymagany wpis dotyczący oferowanego modelu komputera w internetowym katalogu http://www.eu-energystar.org lub http://www.energystar.gov – dopuszcza się wydruk ze strony internetowej – Certyfikat EPEAT na poziomie GOLD Wymagany wpis dotyczący oferowanego modelu komputera w internetowym katalogu http://www.epeat.net - dopuszcza się wydruk ze strony internetowej
<p>Ergonomia</p>	<p>Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego (WORK) wynosząca maksymalnie 23dB (załączyć oświadczenie producenta wraz z raportem badawczym wystawionym przez niezależną akredytowaną jednostkę)</p> <p>Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi.</p>
<p>Warunki gwarancji</p>	<p>5-letnia gwarancja producenta świadczona na miejscu u klienta wraz ze wsparciem technicznym dla fabrycznie zainstalowanych aplikacji; możliwość zgłaszania awarii w trybie 24/7</p> <p>Czas reakcji serwisu - do końca następnego dnia roboczego</p> <p>Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty.</p> <p>Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.</p> <p>W przypadku awarii dysków twardech dysk pozostaje u Zamawiającego – wymagane jest dołączenie do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu o spełnieniu tego warunku.</p>
<p>Wsparcie techniczne producenta</p>	<p>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p> <p>Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera – do oferty należy</p>



	dołączyć link strony.
Wymagania dodatkowe	<ul style="list-style-type: none">- Wbudowane porty: 1 x RS232, 1 x VGA, 2 x PS/2, 1 x DisplayPort v1.1a; 11 szt USB w tym 10 portów USB wyprowadzonych na zewnątrz komputera, port sieciowy RJ-45, porty słuchawek i mikrofonu na przednim oraz tylnym panelu obudowy. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.- Możliwość podłączenia dwóch pracujących równolegle dodatkowych zewnętrznych kart graficznych.- Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika), PXE 2.1;- Płyta główna z wbudowanymi: 1 wolnym złączem PCI 32bit, 2 złączami PCI Express x16 w tym jedno elektrycznie jak PCIe x4; 1 wolnym złączem PCI Express x1; 4 złącza DIMM z obsługą do 16GB DDR3 pamięci RAM, min. 4 złącza SATA w tym 1 szt SATA 3.0;- Klawiatura USB w układzie polski programisty- Mysz optyczna USB z dwoma klawiszami oraz rolką (scroll) min 1000dpi- Nagrywarka DVD +/-RW wraz z oprogramowaniem do nagrywania i odtwarzania płyt- Dołączony nośnik ze sterownikami- Gniazdo GigabitEthernet- Złącze wideo zgodne z oferowanym monitorem (należy dostarczyć kabel do połączenia komputera z monitorem)- Port RS-232- Czytnik kart pamięci obsługujący przynajmniej najbardziej popularne standardy, takie jak: SD, MMC, XD.- 2 porty PS2
Zainstalowany system operacyjny zgodny z wymaganiami	<p>System operacyjny klasy PC musi spełniać następujące wymagania poprzez natywne dla niego mechanizmy, bez użycia dodatkowych aplikacji:</p> <ol style="list-style-type: none">1. Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek;2. Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu;3. Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW;4. Internetowa aktualizacja zapewniona w języku polskim;5. Wbudowana zaporę internetową (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 multimedialny, pomoc, komunikaty systemowe;
7. Wsparcie dla większości 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 z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służąca 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 kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych.
13. Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych.
14. Funkcje związane z obsługą komputerów typu TABLET PC, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego.
15. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika.
16. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
17. Wbudowany system pomocy w języku polskim;
18. Certyfikat producenta oprogramowania na dostarczany sprzęt;
19. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
20. Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji;
21. Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
22. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI



	<p>X.509;</p> <p>23. Wsparcie dla logowania przy pomocy smartcard;</p> <p>24. Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji;</p> <p>25. System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;</p> <p>26. Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach;</p> <p>27. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń;</p> <p>28. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem;</p> <p>29. 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;</p> <p>30. Rozwiązanie ma umożliwiający wdrożenie nowego obrazu poprzez zdalną instalację;</p> <p>31. Graficzne środowisko instalacji i konfiguracji;</p> <p>32. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe;</p> <p>33. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe</p> <p>34. Udostępnianie modemu;</p> <p>35. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej;</p> <p>36. Możliwość przywracania plików systemowych;</p> <p>37. System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.)</p> <p>38. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np przy użyciu numerów identyfikacyjnych sprzętu).</p>
--	--



	<p>39. Koszt połączenia do telefonicznego serwisu technicznego powinien być równoważny co najwyżej połączeniu lokalnemu (inaczej: linii 0-801; preferencja: 0-800, linia bezpłatna dla użytkownika końcowego);</p> <p>40. Telefoniczne wsparcie techniczne w języku polskim w dni robocze od 8:00 do 17:00 zapewniony przez producenta lub dostawcę co najmniej przez 5 lat od chwili zakupu;</p>
--	---

18. Monitory – 100 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne monitora
Typ ekranu	Ekran ciekłokrystaliczny z aktywną matrycą TFT 19" (48,26cm) TN
Rozmiar plamki	0,284 mm
Jasność	250 cd/m ²
Kontrast	1000:1 typowy (50 000:1 dynamiczny)
Kąty widzenia (pion/poziom)	160/160 stopni
Czas reakcji matrycy	max 5ms (czarny do białego)
Rozdzielczość maksymalna	1440 x 900 przy 60Hz
Częstotliwość odświeżania poziomego	30 – 83 kHz
Częstotliwość odświeżania pionowego	56 – 75 Hz
Wydłużenie w pionie	100 mm
Obrót monitora w pionie (PIVOT)	TAK
Obrót monitora w poziomie	+/-45 stopni
Pochylenie monitora	W zakresie od -4 do +21 stopni
Powłoka powierzchni ekranu	Antyodblaskowa
Podświetlenie	System podświetlenia 2 CCFL
Bezpieczeństwo	Monitor musi być wyposażony w tzw. Kensington Slot
Zużycie energii	Max. 50W przy max luminacji, włączonych głośnikach i aktywnych USB Typowe 18W Tryb uśpiący mniej niż 0,5W
Złącze	15-stykowe złącze D-Sub, złącze DVI-D, 4xUSB



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, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. Gwarancja wymiany monitora w przypadku 1 uszkodzonego piksela
Certyfikaty	ISO 13406-2 lub ISO 9241, TCO 5.1, Energy Star 5.0, EPEAT GOLD
Inne	Zdejmowana podstawa oraz otwory montażowe w obudowie VESA 100mm Mozliwość podłączenia do obudowy dedykowanych głośników lub głośniki wbudowane

19. DRUKARKI – 100 SZT.

Wymagane minimalne podstawowe parametry oraz warunki równoważności stawiane zamawianym drukarkom:

Parametr	Wymagane minimalne
Technologia druku	druk laserowy monochromatyczny
Prędkość druku	24 str. A4/min
Czas wydruku pierwszej strony	9 sekund
Rozdzielczość druku	1200x1200 dpi
Podajnik papieru	250 arkuszy 80 g/m ²
Wielofunkcyjny podajnik papieru	1 arkusz
Gramatura obsługiwanych nośników	60-163 g/m ²
Zainstalowana pamięć	64MB
Procesor	360MHz
Porty komunikacyjne	High Speed USB 2.0, Ethernet 10/100 Base TX (wbudowany)
Protokoły sieciowe	TCP/IP, IPSec, IPv6, SNMPv1,2,3, DHCP
Bęben drukujący zintegrowany z tonerem	TAK
Bęben drukujący rozdzielny z tonerem	NIE
Toner	Oryginalny toner producenta urządzenia zintegrowany z bębniem wystarczający do wydrukowania 1000 stron A4 wg normy ISO 19752



Wydajność miesięczna	12,000 str. A4
Maksymalny pobór energii	400W
Gwarancja	nie mniej niż 2 lata gwarancji producenta.

20. Oprogramowanie antywirusowe – 102 szt.

Minimalne wymagania dla oprogramowania antywirusowego stacji roboczych (100 sztuk) oraz serwerów (2 sztuki).

Licencja na okres: 3 lata

Ochrona antywirusowa i antyspyware

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
3. Wbudowana technologia do ochrony przed rootkitami.
4. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
5. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
6. System powinien oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania.
7. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
8. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótów w menu kontekstowym.
9. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
10. Możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Skanowanie plików spakowanych i skompresowanych.
12. Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (w tym z uwzględnieniem plików bez rozszerzeń).
13. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
14. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.



15. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
16. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego).
17. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird i Windows Live Mail
18. 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).
19. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
20. Możliwość definiowania różnych portów dla POP3, na których ma odbywać się skanowanie.
21. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
22. Możliwość skanowania na żądanie lub według harmonogramu baz Outlook Express-a.
23. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
24. 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.
25. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
26. Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie.
27. 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.
28. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.
29. Aktualizacje modułów analizy heurystycznej.
30. 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.



31. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
32. Wysyłanie zagrożeń do laboratorium powinno być możliwe z serwera zdalnego zarządzania i lokalnie z każdej stacji roboczej w przypadku komputerów mobilnych.
33. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń powinny być w pełni anonimowe.
34. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
35. Możliwość automatycznego wysyłania powiadomienia o wykrytych zagrożeniach do dowolnej stacji roboczej w sieci lokalnej.
36. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.
37. Interfejs programu powinien oferować funkcję pracy w trybie bez grafiki gdzie cały interfejs wyświetlany jest w formie formatek i tekstu.
38. Interfejs programu powinien mieć możliwość automatycznego aktywowania trybu bez grafiki w momencie, gdy użytkownik przełączy system Windows w tryb wysokiego kontrastu.
39. Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS i POP3S.
40. Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
41. Administrator powinien mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
42. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.
43. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program powinien pytać o hasło.
44. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji powinno być takie samo.
45. Program powinien być w pełni zgodny z technologią CISCO NAC.
46. Program powinien mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiegś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.
47. Program powinien mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie, powinna także istnieć opcja dezaktywacji tego mechanizmu.
48. Po instalacji programu, użytkownik powinien mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.



49. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB powinien umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
50. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB powinien pracować w trybie graficznym.
51. Program powinien umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: stacji dyskietek, napędów CD/DVD oraz portów USB.
52. Funkcja blokowania portów USB powinna umożliwiać administratorowi zdefiniowanie listy portów USB w komputerze, które nie będą blokowane (wyjątki).
53. Program powinien być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.
54. Funkcja generująca taki log powinna oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.
55. Program powinien oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
56. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
57. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).
58. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
59. 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).
60. Do każdego zadania aktualizacji można przypisać dwa różne profile z innym ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja).
61. Możliwość przypisania 2 profili aktualizacyjnych z różnymi ustawieniami do jednego zadania aktualizacji. Przykładowo, domyślny profil aktualizuje z sieci lokalnej a w przypadku jego niedostępności wybierany jest profil rezerwowo pobierający aktualizację z Internetu.
62. Program wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
63. Praca programu musi być niezauważalna dla użytkownika.
64. Program powinien posiadać dwie wersje interfejsu (standardowy – z ukrytą częścią ustawień oraz zaawansowany – z widocznymi wszystkimi opcjami)
65. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania.
66. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.