



**PROGRAM
REGIONALNY**
NARODOWA STRATEGIA SPÓJNOŚCI



WOJEWÓDZTWO
LUBELSKIE

UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ
ROZWOJU REGIONALNEGO



Zał. nr 10 do SIWZ

PROGRAM FUNKCJONALNO UŻYTKOWY DLA PROJEKTU
KATOLICKIEGO UNIWERSYTETU LUBELSKIEGO IM. JANA PAWŁA II



„SIEC BEZPRZEWODOWA I ELEKTRONICZNY OBIEG SPRAW W KUL”

Lublin, luty 2009

Spis treści

<u>Spis treści.....</u>	<u>2</u>
<u>Projekt techniczny.....</u>	<u>3</u>
<u>System okablowania strukturalnego.....</u>	<u>3</u>
<u>2.1Dopuszcza się każdy system okablowania, dowolnego producenta, spełniający wszystkie</u> <u>poniższe wymagania:.....</u>	<u>5</u>
<u>3. System radiowy</u>	<u>8</u>
<u>3.1 Dopuszcza się każdy system radiowy, dowolnego producenta, spełniający wszystkie poniższe</u> <u>wymagania:.....</u>	<u>9</u>
<u>3.1.1 System zarządzania siecią.....</u>	<u>9</u>
<u>3.1.2 Punkty dostępowe do zastosowań zewnętrznych i wewnętrznych.....</u>	<u>13</u>
<u>3.1.3 Radiolinia</u>	<u>18</u>
<u>4. Dostawa komputerów z dostępem do Internetu:.....</u>	<u>21</u>
<u>5. Dostawa serwerów oraz oprogramowania.</u>	<u>32</u>
<u>5.1 Serwery (2 szt.).....</u>	<u>32</u>
<u>5.2 Macierz (1 szt.).....</u>	<u>35</u>
<u>5.3 System operacyjny (szt. 2).....</u>	<u>37</u>
<u>5.4 Zasilanie awaryjne (szt. 1).....</u>	<u>37</u>
<u>5.5 Agregat prądowórczy trójfazowy (szt. 1).....</u>	<u>38</u>
<u>5.6 Wyposażenie serwerowni oraz wykonane prace (szt. 1).....</u>	<u>39</u>
<u>5.7 Wymagania dotyczące licencji oprogramowania do wirtualizacji.....</u>	<u>40</u>
<u>6. Rozbudowa systemu obiegu spraw</u>	<u>43</u>
<u>7. e-usługi.....</u>	<u>45</u>
<u>Podstawy prawne:.....</u>	<u>46</u>

Projekt techniczny.

Zamawiający wymaga wykonania całości dokumentacji projektowej zarówno dla sieci kablowej jak i 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 (chyba ze nie są wymagane)

Zamawiający wymaga wykonania projektu sieci radiowej w technologii 802.11n zapewniającej podłączenie do Internetu wszystkich pracowników uczelni, studentów i umożliwienie dostępu do Internetu gościa odwiedzającym KUL. Wykonawca zobowiązany jest do wybrania optymalnej lokalizacji stacji nadawczych zapewniającej zasilenie pokrycie 97% wybranych budynków.

Zamawiający wymaga aby projekt wykonany był zgodnie z obowiązującymi przepisami i normami przez osobę mającą uprawnienia w zakresie projektowania sieci.

System okablowania strukturalnego.

Ze względu na wciąż rosnące wymagania prędkościowe i wydajnościowe komputerów oraz aplikacji, coraz mocniej zaznaczające swoją obecność i przydatność usługi multimedialne, a także dynamiczną zmienność charakteru stanowisk końcowych w obiektach/strefach użyteczności publicznej celem dopasowania możliwości obiektu/systemu do zmieniających się wymagań Użytkowników oraz interfejsów i zewnętrznych warunków przyłączeniowych należy zastosować system okablowania strukturalnego jak najbardziej uniwersalny, tj. taki, w którym wszelkiego rodzaju zmiany i rozbudowy będą mogły być samodzielnie prowadzone przez uprawniony personel szybko, a dodatkowo w sposób jak najbardziej prosty i łatwy, bez konieczności prowadzenia poprawek i remontów związanych z ingerencją zewnętrznych grup instalatorskich.

Biorąc pod uwagę aktualną sytuację dotyczącą wydajności systemów okablowania minimalne wymagania dotyczące elementów okablowania strukturalnego to rzeczywista Kategoria 6 / Klasa E oraz RJ45 jako interfejs końcowy dla połączeń na skrętce miedzianej 4 parowej, a dla połączeń światłowodowych kompletny system połączeń zbudowany w oparciu o włókno wielodomowe 50/125µm klasy OM3 oraz standard interfejsu MT-RJ dla sieci światłowodowej.

Dodatkowo, ze względu na charakter obiektu służący różnym grupom użytkowników oraz postęp w dziedzinie technologiach informatycznych, wydajność okablowania ma być gotowa na najnowsze aplikacje – tj. zgodna z ostatnimi wytycznymi komitetów normalizacyjnych oraz najnowszą aktualizacją normy ISO IEC 11801, która określa pasmo przenoszenia dla systemów Klasy E_A/Kategorii 6_A na 500MHz, a pasmo przenoszenia dla systemów Klasy F_A/Kategorii 7_A na 1GHz.

Zamawiający żąda od Wykonawcy przedłożenia oświadczenie potwierdzające kompetencje Wykonawcy do wykonania certyfikowanej instalacji okablowania strukturalnego i o gotowości do

udzielenia 25-letniej gwarancji wydane przez producenta lub dystrybutora oferowanego systemu okablowania, wydane najwcześniej na 3 miesiące przed ogłoszeniem zapytania oraz potwierdzające możliwości i uprawnienia Wykonawcy na rok 2010,

2.1 Dopuszcza się każdy system okablowania, dowolnego producenta, spełniający wszystkie poniższe wymagania:

- Rozwiązanie ma pochodzić od jednego producenta i być objęte jednolitą i spójną gwarancją systemową udzieloną bezpośrednio przez producenta okablowania na okres minimum 25 lat obejmującą wszystkie elementy pasywne toru transmisyjnego, jak również płyty czołowe gniazd końcowych, wieszaki kablowe;
- W celu zagwarantowania Użytkownikowi Końcowemu najwyższej jakości parametrów technicznych i użytkowych cała instalacja musi być nadzorowana w trakcie budowy oraz zweryfikowana przez inżynierów ze strony producenta przed odbiorem technicznym;
- Wszystkie elementy okablowania (w szczególności: kabel, panele krosowe, gniazda, wkładki wymienne, kable krosowe, prowadnice kablowe i inne) mają być oznaczone logo lub nazwą tego samego producenta i pochodzić z jednolitej oferty rynkowej;
- Wszystkie elementy toru transmisyjnego mają być zgodne z wymaganiami obowiązujących norm na min. Kategorię 6_A wg. ISO/IEC 11801 ed. 2.1 z dodatkami Amd.1 (wymagania dla systemu okablowania) i Amd.2 (wymagania dla komponentów) lub EN 50173-1; wydajność komponentów ma być potwierdzona certyfikatem De-Embedded Testing;
- Wydajność systemu okablowania ma być potwierdzona certyfikatem niezależnego laboratorium, np. DELTA, GHMT, itp.;
- System ma się składać z w pełni ekranowanych elementów, szczelnych elektromagnetycznie, tzn. osłoniętych całkowicie (z każdej strony) tzw. klatką Faraday'a; wyprowadzenie kabla ma zapewniać 360° kontakt z ekranem przewodu (to wymaganie dotyczy zarówno gniazd w zestawach ściennych, jak i w panelach krosowych);
- System ma pozwalać na rozbudowę ilości gniazd (interfejsów) końcowych bez konieczności dokładania kabla – jedynie przez wymianę wkładki zakończeniowej* z pojedynczej (np. 1xRJ45) na podwójną (2xRJ45)
- System ma pozwalać na zmianę typu interfejsu dowolnego punktu przyłączeniowego bez zmiany w rozszyciu kabla, tj. poprzez wymianę wkładki zakończeniowej* na odpowiednią w panelu krosowym lub w gnieździe końcowym użytkownika. Budowa systemu ma gwarantować zastosowanie dowolnego interfejsu, który może być wykorzystany zgodnie ze specyfiką pracy obiektu – wśród nich muszą być RJ45, Tera Connector/ISO Cat.7, DB9, RJ12, BNC, złącze F. Zmiana interfejsu końcowego nie może być realizowana za pomocą dodatkowych rozgałęźników czy adapterów – a jedynie przez wymianę wkładki zakończeniowej w gnieździe końcowym.
- System ma pozwalać na zmianę wydajności (kategorii, klasy) okablowania na odpowiednią jedynie przez zmianę wkładek końcowych* - bez zmian kabla transmisyjnego i bez zmian w jego zakończeniu
- System ma mieć możliwość realizacji transmisji wielokanałowej (kilka aplikacji na tym samym kablu) przez wymianę wkładki zakończeniowej*
- System ma być zgodny z obowiązującą specyfikacją Kat.7 i umożliwiać zastosowanie co najmniej 2 rodzajów interfejsów zdefiniowanych przez normę PN-EN 50173-1: 2009.
- W fazie projektowej należy skonfigurować gniazda końcowe tak aby spełniały obecne wymagania kategorii 6/klasy E – wykorzystując we wszystkich gniazdach wkładki 1xRJ45 Kat.6.

Wyjątek stanowią będą niektóre miejsca wskazane po uzgodnieniach z użytkownikiem

- System ma gwarantować przesyłanie sygnału CATV w pełnym paśmie 862MHz oraz integrację transmisji CATV w ramach istniejącej infrastruktury kablowej przez zamontowanie / wymianę wkładki na odpowiednią (z interfejsem typu F) bez konieczności ingerencji w zakończenie kabla.

*Montaż / wymiana wkładki zakończeniowej nie może wymagać ponownej terminacji kabla na złączu.,

- Kable transmisyjne – zgodnie z normą - muszą być zakończone w sposób trwały na 8-pozycyjnym złączu; nie są dopuszczalne zmiany i rekonfiguracje rozszycia w trakcie pracy systemu.
- Ze względów bezpieczeństwa należy zastosować ekranowane kable logiczne 4 parowe o konstrukcji S-FTP (indywidualne ekranowanie każdej pary transmisyjnej folią i dodatkowy ekran wszystkich par z siatki ekranującej). Biorąc pod uwagę przyszłościową rozbudowę, zmiany wydajności do Kat.7_A i możliwości integracji różnych usług w ramach okablowania kable muszą mieć odpowiedni zapas transmisyjny – zastosować kable o paśmie przenoszenia 1200 MHz (lub wyższej) Ze względu na przeznaczenie obiektu kable mają mieć osłonę zewnętrzną niepalną (LSZH).
- W celu zagwarantowania najwyższej jakości połączenia, odpowiedniego marginesu pracy oraz powtarzalnych parametrów, wszystkie złącza, zarówno w gniazdach końcowych jak i panelach muszą być zarabiane za pomocą narzędzi. Ze względu na wymagane parametry oraz niezawodność łączy, nie dopuszcza się złączy zarabianych metodami tzw. beznarzędziowymi. Wymagane są takie rozwiązania, do których montażu stosuje się narzędzia zautomatyzowane (zapewniające jednoczesne zakończenie wszystkich par w jednym ruchu narzędzia, a tym samym powtarzalne i niezmiennie parametry wykonywanych połączeń oraz maksymalnie duże zapasy transmisyjne).
- Maksymalny rozplot pary transmisyjnej na złączu modularnym (umieszczonym w zestawach instalacyjnych i panelach krosowych) nie może być większy niż 6 mm;
- Ekranowane kable krosowe powinny być wykonane z linki typu PiMF w osłonie LSZH o max. średnicy żyły 26 AWG i pozytywnych parametrach transmisyjnych do 600MHz;
- Ekranowane kable krosowe powinny mieć dodatkowe zestyki ekranu, w celu zapewnienia optymalnego kontaktu ekranu kabla z wtykiem i wtyku z gniazdem. Ekran złączy na kablach krosowych powinny zapewnić pełną szczelność elektromagnetyczną z każdej strony złącza. Ze względu na trwałość i niezawodność nie dopuszcza się kabli krosowych z wtykami tzw. zalewanymi;
- System ma mieć możliwość uruchomienia funkcji monitoringu i zarządzania połączeniami fizycznymi w czasie rzeczywistym, poprzez zainstalowanie na panelach sensorowych zestawów uzupełniających i połączenia ich poprzez analizatory sieciowe do relacyjnej otwartej bazy danych. Licencje dostępne do bazy danych mają być bezpłatnie zaimplementowane i udostępnione w analizatorze (urządzeniu monitorującym). Analizatory nie wchodzi w zakres niniejszego zadania.
- W celu zagwarantowania Użytkownikowi Końcowemu najwyższej jakości parametrów technicznych i użytkowych cała instalacja musi być (bezpłatnie) nadzorowana w trakcie budowy

- oraz zweryfikowana przez inżynierów ze strony producenta przed odbiorem techniczny.
- Warunkiem koniecznym dla odbioru końcowego instalacji przez Inwestora jest uzyskanie gwarancji systemowej producenta potwierdzającej weryfikację wszystkich zainstalowanych torów na zgodność parametrów z wymaganiami norm dla Kat.6_A ISO/IEC 11801:2002/Amd.1 i Amd.2:2008.
 - Pomiary wszystkich zainstalowanych torów transmisyjnych muszą zostać wykonane miernikiem, co najmniej poziomu III umożliwiającego pomiar Kat.6_A do 500 MHz. Pomiary torów transmisyjnych muszą wskazywać zgodność wymienionych poniżej parametrów torów z wymaganiami normy ISO/IEC 11801:2002/Amd.1 i Amd.2: 2008 dla Kat.6_A:
 - Do pomiaru należy użyć przystawek do łącza stałego przy ustawieniu ISO/IEC 11801 PL2 lub PL3. Pomiar ma obejmować następujące wielkości:
 - Mapa połączeń
 - Impedancja
 - Rezystancja pętli stałoprądowej
 - Prędkość propagacji
 - Opóźnienie propagacji
 - Tłumienie
 - Zmniejszenie przesłuchu zbliżonego
 - Sumaryczne zmniejszenie przesłuchu zbliżonego
 - Stratność odbiciowa
 - Zmniejszenie przesłuchu zdalnego
 - Zmniejszenie przesłuchu zdalnego w odniesieniu do długości linii transmisyjnej
 - Sumaryczne zmniejszenie przesłuchu zdalnego w odniesieniu do długości linii transmisyjnej
 - Współczynnik tłumienia w odniesieniu do zmniejszenia przesłuchu
 - Sumaryczny współczynnik tłumienia w odniesieniu do zmniejszenia przesłuchu

3. System radiowy

System ma obić swym zasięgiem cały obszar należący do Katolickiego Uniwersytetu Lubelskiego w Lublinie na osiedlu Majdanek tj budynki numer 1,2,3, 5, 48 i 52 oraz budynek biblioteki uniwersyteckiej przy ul. Chopina.

W przypadku sieci na osiedlu Majdanego zamawiający wymaga wykonania sieci zarówno w budynkach jak i przed budynkami tak aby objąć zasięgiem cały teren należący do KUL.

W przypadku biblioteki uniwersyteckiej zasięgiem sieci należy objąć cały budynek + najbliższe okolice (zakłada się promień około 100 metrów od budynku)

Wszystkie działania związane z realizacją zadania będą realizowane zgodnie z głównym celem projektu jakim jest:

- a) Zapewnienie dostępu do sieci lokalnej (intranet) jaki i Internetu dla pracowników KUL,
- b) Zapewnienie dostępu do sieci lokalnej (intranet) jaki i Internetu dla studentów KUL,
- c) Zapewnienie dostępu do sieci Internet oraz wybranych stref sieci lokalnej dla gości KUL,

Realizacja działań spełniać będzie normy branżowe i standardy przewidziane obowiązującymi przepisami. Musi być realizowana zgodnie z obowiązującym prawem. Zamawiający żąda od Wykonawcy oświadczenie potwierdzające kompetencje Wykonawcy do budowy sieci bezprzewodowej, wydane najwcześniej na 3 miesiące przed ogłoszeniem postępowania oraz potwierdzające możliwości i uprawnienia wykonawcy na rok 2010.

3.1 Dopuszcza się każdy system radiowy, dowolnego producenta, spełniający wszystkie poniższe wymagania:

3.1.1 System 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 urządzenia do systemu monitoringu sieci.

Lp.	Obszar	Wymagania
1	Zarządzanie użytkownikami	<ul style="list-style-type: none">• 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

		<p>ustawienia wyższego priorytetu dla wskazanych portów bezpośrednio w ramach kolejki użytkownika</p> <ul style="list-style-type: none"> • 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.)
--	--	--

		<ul style="list-style-type: none"> • 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 ustawy o obowiązkach 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	<ul style="list-style-type: none"> • Graficzny interfejs podglądu Sieci z poziomu www • Przedstawienie wszystkich elementów Sieci w na mapie graficznej • Podgląd wszystkich logów urządzeń w systemie • Zbieranie logów i zapisywanie w bazie danych • Możliwość naniesienia na mapę innych urządzeń • Możliwość naniesienia na mapę przebiegów tras kabli

		<p>światłowodowych</p> <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 RADIUS AAA • Telefonía IP • Zdalna administracja winbox GUI • Konfiguracja za pomocą telnetu, ssh lub portu szeregowego <p>• Konfiguracja i monitorowanie w czasie rzeczywistym</p>

3.1.2 Punkty dostępowe do zastosowań zewnętrznych i wewnętrznych

Lp.	Element	Wymagania
1.	Płyta główna	<ul style="list-style-type: none"> • Procesor - MPC854 800MHz • Pamięć - 256MB DDR2 SDRAM • Bios - RouterBOOT • Dysk - 64MB pamięci NAND na stałe wbudowane w płytę lub złącze CF • Port LAN - 3x10/100/1000 Mbit/s Gigabit ethernet z obsługą Auto-MDI/X • Sloty miniPCI - 3x MiniPCI + 1x miniPCI-e • port rozszerzeń PCI-e • Beeper - tak • Port szeregowy - jeden DB9 RS232C, standardowo 115200bps 8N1 • Diody LED - 1x zasilanie, 1x użytkownika • Zasilanie - PoE 36V-56V DC lub gniazdo zasilające DC 10-56V • Wymiary - 14 cm x 20 cm <ul style="list-style-type: none"> • System Mikrotik OS z licencją Level6.
2.	Karta radiowa 2 szt. dla każdego zestawu.	<p>Podstawowe cechy:</p> <ul style="list-style-type: none"> • Turbo, 802.11a, 802.11b/g w jednej karcie • Pracuje w obu 2.4 and 5Ghz pasmach • Zgodna z CE i FCC • Pracuje w zakresie 2.192-2.539 oraz 4.920-6.100GHz i obsługuje tryb Turbo. <p>Dane techniczne:</p> <ul style="list-style-type: none"> • Chipset: Atheros AR5414 • Standardy: IEEE802.11a/b/g • Media Access: CSMA/CA with ACK architecture 32-bit MAC • Bezpieczeństwo: szyfrowanie 64/128bit WEP, TKIP, AES-CCM, 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 • Złącza: 2x uFI • Zasilanie: 3.3V +/-10%, 800mA max, typ 600mA • Częstotliwości: 2.192-2.539 and 4.920-6.100GHz • Moc wyjściowa/Czułość: <ul style="list-style-type: none"> 802.11a - 24dBm/-90dBm@6Mbps, 19dBm/-70dBm@54Mbps 802.11b - 25dBm/-92dbm@1Mbps, 25dBm/-87dBm@11Mbps 802.11g - 25dBm/-90dBm@6Mbps, 20dBm/-

		<p>70dBm@54Mbps</p> <ul style="list-style-type: none"> • Temperatura pracy: -20 to 70C • Temperatura przechowywania: -65 to 100C • Dopuszczalna wilgotność: 5% - 95 %
3	Karta radiowa	<p>karta miniPCI pracując w standardzie 802.11N potrafi osiągnąć pięciu krotnie wyższe prędkości od standardów 802.11A/B... jednak wciąż jest z nimi kompatybilna. Pracując w standardzie 802.11N karta wykorzystuje technologie MIMO (Multiple-input multiple-output) czyli nadawanie/odbieranie trzema antenami jednocześnie.</p> <p>Dane techniczne:</p> <ul style="list-style-type: none"> • Chipset Atheros AR9160 • Modulacja 802.11b/g 5.5/11 Mbps(CCK),2 Mbps(DQPSK),1 Mbps(DBPSK) • Modulacja 802.11a 48/54 Mbps(QAM-64),24/36 Mbps(QAM-16),12/18 Mbps(QPSK),6/9Mbps (BPSK) • Modulacja 802.11n QAM-64,QAM-16,QPSK,BPSK • Standard interfejsu 32-bit mini-PCI, Type IIIA • Pasmo 802.11b/g 2.412-2.472GHz • Pasmo 802.11a/n 5.150-5.350GHz; 5.475-5.725GHz; 5.725-5.850GHz • Napięcie pracy 3.3V +/- 5% • Wymiary 59.7mm x 44.6mm x 5 mm Waga 20g • Temperatura pracy 0°C do 50°C • Temperatura magazynowania -20°C do 85°C • Wyjście antenowe 3 x U.fl Gwarancja 12 miesięcy
4.	Obudowa	<p>Specyfikacja:</p> <ul style="list-style-type: none"> – wykonanie obudowy - odlew aluminiowy malowany proszkowo – klasa szczelności IP65 (uszczelka) – zawiasy dla łatwego otwierania – montaż na ścianie lub maszcie o średnicy do 55 mm – 4x otwory średnicy 16mm do wyprowadzenia konektorów – 1x otwór na przepust elektryczny <p>Wyposażenie:</p> <ul style="list-style-type: none"> – obudowa – 2x uchwyty do przykręcenia do masztu lub ściany – 2x zaślepki – 1x przepust elektryczny PG9 – 1x płyta montażowa z otworami i śrubami – 8x dystanse, nakrętki i śruby do przykręcenia płyt
4.	Zasilacz buforowy	Parametry techniczne:

		<ul style="list-style-type: none"> • 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 zwarciove
5.	System Operacyjny	<p>Funkcje bezprzewodowego punktu dostępowego:</p> <ul style="list-style-type: none"> • 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 <p>Podstawowe cechy systemu:</p> <ul style="list-style-type: none"> • 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, IP/IP), VLAN, PPPoE • Mosty STP z filtrowaniem pakietów • Equal cost multi path routing • Policy based routing <p>Funkcjonalność "Plug and Play":</p> <ul style="list-style-type: none"> • HotSpot z autentykacją RADIUS • Uniwersalny Klient • DHCP - serwer i relay • Protokół Univesal Plug and Play (UpnP) • Protokoły RIP, OSPF i BGP <p>Zarządzanie:</p> <ul style="list-style-type: none"> • 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

		<p>Ograniczenia licencji:</p> <ul style="list-style-type: none"> • liczba tuneli PPPoE, PPTP, L2TP – bez ograniczeń • liczba jednocześnie obsługiwanych klientów Hot-Spot – bez ograniczeń
8	Antena 5,5 GHz – omni – 4 sztuki	<ul style="list-style-type: none"> • Typ anteny: dookólna • Zakres częstotliwości: 5,47 - 5,875 GHz • Zysk energetyczny: 11,3 dBi • Polaryzacja: pionowa • Kąt promieniowania w płaszczyźnie pionowej: 8 ° dla -3dB • VSWR: 1 do 1,5 • Impedancja: 50 Ohm • Złącze: N/Żeńskie • Montaż: do masztu lub obudowy • Wymiary: 22 x 480 mm
10	Antena 2,4 GHz – omni – 1 sztuka	<ul style="list-style-type: none"> • Typ anteny: dookólna • Zakres częstotliwości : 2,4 - 2,5 GHz • Zysk energetyczny: 10 dBi • Polaryzacja: pionowa • Kąt promieniowania w płaszczyźnie pionowej: 23 ° • Kąt promieniowania w płaszczyźnie poziomej: 360 ° • VSWR: 1 do 1,5 • Impedancja: 50 Ohm • Złącze: N/Żeńskie • Montaż: do masztu lub obudowy • Wymiary: 675 x fi 22 mm

Zakres prac do wykonania

- Podłączenia jak największej ilości punktów dostępowych do sieci kablowej
- W przypadku braku możliwości podłączenia danego punktu do sieci kablowej skonfigurować dla punktów dostępowych sieć MASH w oparciu o pasmo 5 GHz
- Podłączenia do serwera zarządzającego przy pomocy dedykowanego VLAN-a
- W przypadku przekroczenia wysokości masztu > 3 metrów wykonanie dokumentacji i zgłoszenia robót budowlanych,

- Instalacje masztu antenowego na dachu budynku (kratownica),
- Instalacje konstrukcji podantenowej,
- Instalacje anten,
- Instalacje urządzeń,
- Uruchomienie i konfiguracja urządzeń (uruchomienie usługi),
- Przygotowanie dokumentacji powykonawczej.

Lokalizacje stacji nadawczych

Lokalizacje zostaną wybrane przez Wykonawcę i umieszczone w projekcie w porozumieniu z Zamawiającym

Usługi serwisowe dla stacji nadawczych

Wykonawca zapewni dla dostarczonych i uruchomionych stacji nadawczych usługi serwisowe przez okres 36 miesięcy, począwszy od dnia oddania sieci do eksploatacji (podpisania protokołu odbioru przez Zamawiającego). Awaryjne stacji nadawczych będą usuwane przez Wykonawcę w ciągu 24 godzin od otrzymania zgłoszenia.

Kompleksowość instalacji

Zamawiający wymaga dostarczenia i uruchomienia całości sieci oraz konfiguracji urządzeń i integracji z istniejącą infrastrukturą zamawiającego.

3.1.3 Radiolinia

Zamawiający wymaga dostawy i uruchomienia linii radiowej (w relacji Budynek główny KUL – Majdanek)

- Radiolinia powinna pracować w pasmach licencjonowanych od 6GHz do 38GHz
- System powinien posiadać budowę typu, Split, czyli jednostkę Indoorową (IDU) i Outdoorową (ODU). Jednostka Indoorowa powinna być niezależna od częstotliwości.
- System powinien oferować dwukierunkową transmisję z przepływnościami od 4Mbps do powyżej 690Mbps.
- System powinien oferować transport dla technologii Ethernet oraz PDH, ze wsparciem interfejsów SDH.
- System powinien oferować ACAP, ACCP oraz CCDP niezależnie od technologii (Ethernet, PDH, SDH).
- System powinien oferować możliwość transportu STM-1 z modulacją 16, 64 oraz 128 QAM.
- System powinien oferować możliwość transportu Ethernetu i PDH w jednym łączy w postaci natywnej z możliwością konfiguracji z krokiem 2Mbps (E1).
- System powinien oferować możliwość pracy w trybie bez protekcji 1+0 oraz z protekcją mikrofalową typu 1+1.
- System powinien oferować możliwość pracy z protekcją typu 2+0 dla ruchu hybrydowego (Ethernet oraz PDH). Dostawca powinien opisać metody protekcji ruchu.
- System powinien oferować możliwość transportu ramek Ethernetowych do rozmiaru 2000 Byte zgodnie z IEEE 802.as.
- INDOOR UNIT (IDU)
- System powinien oferować możliwość krosowania sygnałów na poziomie E1 pomiędzy kartami na wewnętrznej matrycy krosującej. Maksymalna pojemność matrycy powinna być podana.
- Jednostka indoorowa powinna oferować możliwość zaterminowania sygnału STM-1, oraz dalszy transport sygnałów w postaci nxE1 poprzez wewnętrzną matrycę krosującą bez użycia zewnętrznych kabli.
- Jednostka indoorowa powinna oferować możliwość protekcji w ringu E1 1+1 SNCP.

- Interfejs STM-1 powinien oferować możliwość pracy z protekcją MSP 1+1
- Zarządzanie radiolinią (sieć DCN) powinno wykorzystywać technologię IP.
- Jednostka indoorowa powinna oferować możliwość podłączenia poniższych interfejsów:
 - 10BASE-T
 - 100BASE-TX
 - 1000BASE-T
 - 1000BASE-LX
 - 1000BASE-ZX
- Zgodnie z IEEE 802.3u, 802.3ab oraz 802.3z
- System powinien oferować możliwość wykorzystania wkładek SFP dla interfejsów GE (Gigabit Ethernet) zarówno elektrycznych oraz optycznych.
- Interfejsy Ethernetowe powinny oferować możliwość pracy z protekcją LAG (Link Aggregation Group).
- System powinien oferować możliwość wsparcia dla Class of Service (CoS) zgodnie z IEEE 802.1p.
- System powinien oferować możliwość obsługi 8 klas usług (8 kolejek wg. IEEE 802.1 D lub 802.1Q).
- System powinien oferować możliwość obsługi QoS na podstawie informacji zawartych w ramce Ethernetowej (PCP), IP (DSCP) lub MPLS (EXP).
- System powinien oferować Ethernet Link O&M.

- ETHERNET SWITCHING
 - System powinien oferować zbudowany Ethernet Switch zgodny z 802.1Q-2005.
 - Wbudowany Ethernet Switch powinien oferować przynajmniej 10 portów.
 - Wbudowany Ethernet Switch powinien oferować funkcjonalność Provider Bridge zgodną z IEEE 802.1ad, obecnie lub po software upgrade.

- ETHERNET
 - System powinien oferować transport natywnego Ethernetu w kanałach od 7 do 56MHz z przepływnością od 4Mbps do 690Mbps.

Przy System powinien oferować możliwość zdublowania przepływności łącza Ethernetowego poprzez wykorzystanie dwóch polaryzacji w jednym kanale pracujących w oparciu o funkcjonalność XPIC.

- MODULACJA ADAPTACYJNA

System powinien oferować bezprzerwową modulację adaptacyjną, która będzie zależna od warunków propagacyjnych.

Modulacja Adaptacyjna powinna być w zakresie od 4 do 256QAM dla łączy pracujących bez XPIC.

Modulacja Adaptacyjna powinna być dostępna w kanałach 7, 14, 28, 40 i 56MHz.

Zmiany schematu modulacji w funkcjonalności Modulacji Adaptacyjnej powinny następować bez przerwy w ruchu zarówno dla części PDH jak i części ruchu Ethernet o wysokim priorytecie oraz ze stałym opóźnieniem.

- OUTDOOR UNIT (ODU)

Jednostka outdoorowa powinna być uniwersalna i niezmienna dla wszelkich przepływności czy zastosowanych modulacji.

- ANTENA

System powinien oferować anteny paraboliczne gotowe do montażu zintegrowanego dla średnic od 0,2m do 1,8m włącznie.

4. Dostawa komputerów z dostępem do Internetu:

Zamawiający wymaga dostawy 14 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	<ul style="list-style-type: none"> - 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 (oczeko 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: <ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> - 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

		<p>do niego, urządzeń zewnętrznych , informacji na temat: zainstalowanego procesora, pamięci operacyjnej RAM wraz z informacją o obsadzeniu slotów pamięci, obsadzeniu slotów PCI.</p> <ul style="list-style-type: none"> - 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 wyłączenia 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	<ul style="list-style-type: none"> - 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	<p>5-letnia gwarancja producenta świadczona na miejscu u klienta Czas reakcji serwisu - do końca następnego dnia roboczego. Gwarancja na</p>

	monitorem	<p>sprzet orza oprogramowanie fabrycznie zainstalowane na komputerze.</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 gwarancyjnym.</p>
18.	Inne	<p>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p> <p>Dołączony nośnik ze sterownikami.</p>
	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 KUL
- 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	<p>Pełne wsparcie dla systemu Windows 2000/2003/XP/PC Tablet/Vista/2008.</p> <p>Wsparcie dla Windows Security Center (Windows XP SP2).</p> <p>Wsparcie dla 32- i 64-bitwej wersji systemu Windows.</p> <p>Wersja programu dla stacji roboczych Windows dostępna zarówno języku polskim jak i angielskim.</p> <p>Pomoc w programie (help) w języku polskim.</p>

		<p>Dokumentacja do programu dostępna w języku polskim.</p> <p>Skuteczność programu potwierdzona nagrodami VB100 i co najmniej dwie inne niezależne organizacje np. ICSA labs lub Check Mark.</p>
2.	Ochrona antywirusowa i antyspyware	<p>Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.</p> <p>Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.</p> <p>Wbudowana technologia do ochrony przed rootkitami.</p> <p>Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.</p> <p>Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.</p> <p>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).</p> <p>Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.</p> <p>Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.</p> <p>Możliwość skanowania dysków sieciowych i dysków przenośnych.</p> <p>Skanowanie plików spakowanych i skompresowanych.</p> <p>Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (w tym z uwzględnieniem plików bez rozszerzeń).</p> <p>Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.</p> <p>Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.</p> <p>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.</p> <p>Wbudowany konektor dla programów MS Outlook, Outlook Express i Windows Mail (funkcje programu dostępne są bezpośrednio z menu</p>

	<p>programu pocztowego).</p> <p>Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook.</p> <p>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).</p> <p>Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.</p> <p>Możliwość definiowania różnych portów dla POP3, na których ma odbywać się skanowanie.</p> <p>Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.</p> <p>Możliwość skanowania na żądanie lub według harmonogramu baz Outlook Express-a.</p> <p>Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.</p> <p>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.</p> <p>Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.</p> <p>Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie..</p> <p>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.</p> <p>Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz</p>
--	---

	<p>wirusów.</p> <p>Inkrementacyjne aktualizacje modułów analizy heurystycznej.</p> <p>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.</p> <p>Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.</p> <p>Wysyłanie zagrożeń do laboratorium powinno być możliwe z serwera zdalnego zarządzania i lokalnie z każdej stacji roboczej w przypadku komputerów mobilnych.</p> <p>Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń powinny być w pełni anonimowe.</p> <p>Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.</p> <p>Możliwość automatycznego wysyłania powiadomienia o wykrytych zagrożeniach do dowolnej stacji roboczej w sieci lokalnej.</p> <p>W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e mail.</p> <p>Możliwość zabezpieczenia hasłem dostępu do opcji konfiguracyjnych programu.</p> <p>Możliwość zabezpieczenia hasłem możliwości wyłączenia programu antywirusowego i poszczególnych funkcji programu</p> <p>Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.</p> <p>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).</p> <p>Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.</p> <p>Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po</p>
--	---

		<p>zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja).</p> <p>Możliwość określenia częstotliwości aktualizacji w odstępach 1 minutowych.</p> <p>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.</p> <p>Program wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, antyspam).</p> <p>Praca programu musi być niezauważalna dla użytkownika.</p> <p>Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania.</p>
3.	Ochrona przed spamem	<p>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.</p> <p>Pełna integracja z programami pocztowymi MS Outlook, Outlook Express i Windows Mail – antyspamowe funkcje programu dostępne są bezpośrednio z menu programu pocztowego.</p> <p>Automatyczne wpisanie do białej listy wszystkich kontaktów z skrzynki adresowej programu pocztowego.</p> <p>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.</p>
4.	Zapora osobista (personal firewall)	<p>Zapora osobista mogąca pracować jednym z 3 trybów:</p> <ul style="list-style-type: none"> - 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

		<p>przepuszczany.</p> <p>Możliwość tworzenia list sieci zaufanych.</p> <p>Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.</p> <p>Możliwość wyboru jednej z 3 akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj o decyzję.</p> <p>Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń.</p> <p>Możliwość zdefiniowania 2 oddzielnych zestawów reguł – jeden dla strefy zaufanej (sieć wewnętrzna) i drugi niezauwanej (internet).</p> <p>Wbudowany system IDS.</p> <p>Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu.</p>
5.	Zdalna konsola administracyjna	<p>Centralna instalacja i zarządzanie wszystkimi programami na stacjach roboczych Windows i serwerach Windows.</p> <p>Zdalna instalacja wszystkich wersji programu na stacjach roboczych Windows NT/2000/XP Professional/PC Tablet/ Vista.</p> <p>Do instalacji zdalnej i zarządzania zdalnego nie jest wymagany dodatkowy agent. Na końcówkach zainstalowany jest sam program antywirusowy</p> <p>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</p> <p>Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych z opcją wygenerowania raportu ze skanowania i przesłania do konsoli zarządzającej.</p> <p>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).</p> <p>Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, adresów MAC, wersji systemu operacyjnego oraz domeny, do której</p>

		<p>dana stacja robocza należy.</p> <p>Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub internetu.</p> <p>Możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych.</p> <p>Możliwość tworzenia grup stacji roboczych i definiowania w ramach grupy wspólnych ustawień konfiguracyjnymi dla zarządzanych programów.</p> <p>Możliwość importowania konfiguracji programu z wybranej stacji roboczej a następnie przesłanie (skopiowanie) jej na inną stację lub grupę stacji roboczych w sieci.</p> <p>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).</p> <p>Możliwość uruchomienia serwera zdalnej administracji na stacjach Windows NT/XP/2000 oraz na serwerach Windows NT 4.0/2000/2003.</p> <p>Możliwość uruchomienia centralnej konsoli zarządzającej na stacji roboczej Windows 98/ME/NT/2000/XP.</p> <p>Możliwość wymuszenia konieczności uwierzytelniania stacji roboczych przed połączeniem się z serwerem zarządzającym. Uwierzytelnianie przy pomocy zdefiniowanego na serwerze hasła.</p> <p>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.</p> <p>Do instalacji serwera centralnej administracji nie jest wymagane zainstalowanie dodatkowych aplikacji takich jak Internet Information Service (IIS) czy Apache.</p> <p>Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) w formacie HTML lub CSV.</p> <p>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).</p> <p>Możliwość tworzenia repozytorium aktualizacji na serwerze centralnego</p>
--	--	---

		zarządzania i udostępniania go przez wbudowany serwer http.
--	--	---

5. Dostawa serwerów oraz oprogramowania.

5.1 Serwery (2 szt.)

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, umożliwiającą 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	<p>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.</p> <p>W przypadku zaferowania 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.</p>
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 baterijnym, 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: <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
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 slotcie karta zarządzająca niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane złącze RJ-45 i umożliwiające: <ul style="list-style-type: none"> ▪ 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 autentykację 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 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	<p>Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001.</p> <p>Deklaracja CE.</p> <p>Serwer musi spełniać normy Energy Star 1.0 for Computer Servers.</p> <p>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.</p> <p>Wymagane jest dostarczenie odpowiednich certyfikatów.</p>
Warunki gwarancji	<p>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.</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> <p>Zamawiający oczekuje fizycznej instalacji i testów uruchomieniowych oferowanych serwerów.</p> <p>Zamawiający oczekuje możliwości przedłużenia czasu gwarancji do pięciu lat.</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>

5.2 Macierz (1 szt.)

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.

5.3 System operacyjny (szt. 2)

MS Windows Server Standard 2008

5.4 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.

5.5 Agregat prądowórczy trójfazowy (szt. 1)

Dostawa i instalacja urządzenia o następujących minimalnych parametrach:

- Czas pracy na pełnym zbiorniku (godz.) 8
- Częstotliwość (Hz) 50
- Ilość faz Trójfazowy
- Ilość pól prądnicy 4
- Moc maksymalna (kVA) 40.0
- Moc nominalna (kVA) 37.0
- Moc prądu stałego (V/A)
- Napięcie (V) 230/400
- Obroty (rpm) 1500
- Paliwo ON
- Podłączenie automatyki
- Pojemność miski olejowej (l) 11
- Pojemność zbiornika paliwa (l) 95
- Poziom hałasu dB(A) z odl. 7m 51
- Prąd (A) 53.4
- Rodzaj oleju Olej mineralny 15W40
- Silnik KIPOR
- Silnik-Moc nominalna [kW(Hp)/rpm] 41.6/1500
- Silnik-pojemność (cm³) 4329
- Silnik-typ Czterocylindrowy, 4-suwowy, chłodzony cieczą, silnik Diesla
- Struktura Zabudowany, bardzo cichy
- System kontroli Samokontrola i stabilizacja napięcia (AVR)
- System rozruchowy Elektryczny
- Średnica cylindra x skok tłoku (mm) 105 x 125
- Waga netto (kg) 1100
- Współczynnik mocy (cos) 0.8
- Wymiary /dł. x szer. x wys./ (mm) 2250 x 950 x 1300
- Zużycie paliwa (g/kWh) <300
- Dostawa ATS (Automatycznego systemu sterowania)

5.6 Wyposażenie serwerowni oraz wykonane prace (szt. 1)

- Wymagane jest dostarczenie szafy serwerowej o wymiarach szerokość min. 600mm, głębokość min. 1000mm , wysokość minimalnie 25U , kolor czarny.
- Dostawa wszystkich niezbędnych elementów do uruchomienia dostarczonego sprzętu.
- 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.

5.7 Wymagania dotyczące licencji oprogramowania do wirtualizacji

Licencje powinny umożliwiać uruchomienie 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 umożliwić 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.

6. Rozbudowa systemu obiegu spraw

Zamknięty Serwis społeczności studentów i pracowników: e-KUL w zakresie:

Rozwinięcia systemu obiegu spraw i dokumentów w zakresie spraw wewnętrznych (WEB S4A)

6.1 Sprawy studenckie:

- zapisywanie na zajęcia dydaktyczne,
- wnioski stypendialne,
- wniosek o zatwierdzenie tematu pracy dyplomowej, przesunięcie terminu, przygotowania pracy w języku obcym,
- obsługa płatności w tym wnioski o zwolnienia,
- wnioski w sprawach toku studiów (bierne w S4A)
- wnioski o urlopy zdrowotne i okolicznościowe,
- wnioski o zmianę w organizacji studiów (IOS, ITS),
- wnioski o zgodę na powtarzanie przedmiotu, odbycie egzaminu komisyjnego lub etapu studiów
- wnioski o zmianę specjalizacji,
- wnioski o zgodę na II fakultet,
- wnioski o oddelegowanie etapu studiów do innej Uczelni (MOST)
- wnioski o duplikaty dokumentów,
- wnioski o zmianę danych osobowych lub adresowych,
- wnioski o wydanie odpisu dyplomu, dyplomu w języku obcym
- wnioski o wydanie zaświadczeń,

6.2 Sprawy pracownicze:

- obsługa rachunków do umów cywilno-prawnych,
- obsługa zapotrzebowań na towary i usługi,
- wnioski o delegacje,
- wnioski o urlopy,

- wnioski (bierne w S4A)
- wnioski o wydanie zaświadczeń,
- wnioski o zapomogi,
- wnioski o zmianę danych osobowych lub adresowych,

6.3 Budowy systemu prezentacji informacji z S4A w zakresie:

- wewnętrznych aktów prawnych,
- stanu finansowego prowadzonych projektów ,
- stanu wykonania budżetu.

7. e-usługi

Zamawiający wymaga budowy systemu obsługi spraw w zakresie obsługi klientów zewnętrznych (skrzynka podawcza WEB S4A)

Rozwój systemu e-learning w zakresie treści podniesienie jakości istniejących kursów

Akceptuję bez zastrzeżeń:

.....
*(podpis i pieczęć upoważnionego
przedstawiciela wykonawcy)*

Podstawy prawne:

- Ustawa Prawo Budowlane z dnia 7 lipca 1994r. (tekst jednolity Dz. U. z 2006r. Nr 156, poz. 1118, Nr 170, poz. 1217),
- Rozporządzenie Ministra Infrastruktury z dnia 2 września 2004 roku w sprawie szczegółowego zakresu i formy dokumentacji projektowej, specyfikacji technicznych wykonania i odbioru robót budowlanych oraz programu funkcjonalno-użytkowego (Dz.U. Nr 202 poz.2072),
- Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 26 września 1997r. w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy (tekst jednolity Dz. U. z 2003r. Nr 169 poz.1650),
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 4 listopada 2002r. w sprawie organizacji, zasad i trybu wykonywania zadań przez Państwową Inspekcję Sanitarną MSWiA (Dz. U. Nr 192, poz. 1614) - §1, §2, §3 pkt. 1,
- Rozporządzenie Ministra Spraw Wewnętrznych i administracji z dnia 16 czerwca 2003r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz. U. z 2003r.nr 121 poz.1138),
- Rozporządzenie Ministra Spraw Wewnętrznych i administracji z dnia 16 czerwca 2003r. w sprawie uzgadniania projektu budowlanego pod względem ochrony przeciwpożarowej (Dz. U. z 2003r.nr 121 poz.1137),
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 21 kwietnia 2006r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz. U. Nr 80, poz. 563).