Projekt współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego
w ramach Programu Operacyjnego Innowacyjna Gospodarka
„Dotacje na Innowacje" „Inwestujemy w Wasza przyszłość"

SR.271.2.2011

Załącznik nr 1 do umowy

Opis przedmiotu zamówienia

1. Komputery stacjonarne: 41 szt.

Lp.	*Nazwa komponentu*	*Wymagane minimalne parametry techniczne sprzętu*
1.	Typ	Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
2.	Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna
3.	Wydajność obliczeniowa	Komputer powinien osiągać w teście wydajności PassMark Performance Test 7.0 CPU Mark wynik min. 3830 punktów. W dniu dostawy Zamawiający przeprowadzi test wydajności na dwóch losowo wybranych zestawach, w celu weryfikacji zgodności dostarczonego sprzętu z zamówieniem. Wyniki testów będą wydrukowane i potwierdzone przez obie strony.
4.	Pamięć operacyjna	min. 4GB możliwość rozbudowy do min. 16GB, dwa sloty wolne
5.	Parametry pamięci masowej	min. 250 GB SATA, podzielony na dwie zbliżone pojemnościowo partycje
6.	Wydajność grafiki	Grafika powinna umożliwiać pracę 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
7.	Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, Porty słuchawek i mikrofonu na przednim oraz na tylnym panelu obudowy.
8.	Obudowa	Typu desktop z obsługą kart PCI 32bit oraz PCI Express, fabrycznie przystosowana do pracy w układzie pionowym i poziomym, oraz możliwością postawienia na obudowie w pozycji poziomej monitora; wyposażona w min. 2 kieszenie: 1 szt 5,25" zewnętrzne i 1 szt 3,5" wewnętrzne. W celu szybkiej weryfikacji usterki w obudowę komputera musi być wbudowany wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami; a w szczególności musi sygnalizować:

		• Przebieg procesu POST • Awarię BIOS-u • Awarię procesora • Uszkodzenia lub braku pamięci RAM, uszkodzenia złączy PCI i PCIe, kontrolera Video, płyty głównej, kontrolera USB
9.	Zgodność z systemami operacyjnymi i standardami	Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z systemem operacyjnym Windows 7 32bit i 64bit **(załączyć do oferty wydruk ze strony Microsoft WHCL).**
10.	Dodatkowe oprogramowanie	Oprogramowanie dostarczone przez producenta komputera pozwalające na zdalną inwentaryzację komputerów w sieci, lokalną i zdalną inwentaryzację komponentów komputera, umożliwiające co najmniej: • informowanie administratora o otwarciu obudowy, • zdalne zablokowanie stacji dysków, portów szeregowych, równoległych, USB, • zdalne uaktualnianie BIOS zarówno na pojedynczym komputerze a także na grupie komputerów w tym samym czasie, • zdalną konfigurację BIOS w czasie rzeczywistym, w tym co najmniej ustawienie hasła, wpisanie unikalnego numeru nadanego przez użytkownika, sekwencji startowej, włączenia/wyłączenia portów USB, włączenia/wyłączenia karty dźwiękowej, • zdalne wyłączanie oraz restart komputera w sieci, • otrzymywanie informacji WMI – Windows Management Interface, • monitorowanie stanu komponentów: CPU, Pamięć RAM, HDD, wersje BIOS • monitorowanie i alertowanie parametrów termicznych, wolnego miejsca na dyskach twardych. • monitorowanie stanu komponentów: CPU, Pamięć RAM, HDD, wersje BIOS przy wyłączonym komputerze lub nieobecnym/uszkodzonym systemie operacyjnym, • zdalne przejęcie konsoli tekstowej stacji roboczej przy wyłączonym komputerze lub nieobecnym/uszkodzonym systemie operacyjnym, Musi umożliwiać ustawienie sposobu informowania o zaistnieniu zdarzenia poprzez (po stronie serwera) automatyczne uruchomienie zaplanowanej wcześniej akcji, wysłanie raportu zawierającego między innymi numer seryjny komputera i opis błędu na wskazany adres poczty elektronicznej.
11.	Certyfikaty i standardy	• Certyfikat ISO9001 dla producenta sprzętu **(załączyć do oferty dokument potwierdzający spełnianie wymogu)** • Deklaracja zgodności CE **(załączyć do oferty dokument potwierdzający spełnianie wymogu)** • Komputer musi spełniać wymogi normy Energy Star 5.0 **(załączyć do oferty dokument potwierdzający spełnianie wymogu)**
12.	Ergonomia	Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń, napędu optycznego i 3,5” dysku twardego 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) oraz powinna posiadać czujnik otwarcia obudowy współpracujący z

		oprogramowaniem zarządzająco – diagnostycznym producenta komputera; Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) oraz kłódki (oczko w obudowie do założenia kłódki); Obudowa musi być wyposażona w zamek który nie wystaje poza obrys obudowy.
13.	Warunki gwarancji	60-miesięczna gwarancja producenta świadczona na miejscu u klienta. Czas reakcji serwisu - do końca następnego dnia roboczego od dnia zgłoszenia usterki. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – **(załączyć do oferty dokument potwierdzający spełnianie wymogu).** Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.
14.	Wsparcie techniczne producenta	Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera.
15.	Wymagania dodatkowe	1. Zainstalowany system operacyjny Windows 7 Professional 64bit PL z SP 1 (licencję dostarcza Wykonawca) + nośnik z systemem operacyjnym lub system równoważny 2. Wbudowane porty: 1 x RS232, 1 x VGA, 2 x PS/2, 1 x DisplayPort v1.1a; min. 8 portów USB wyprowadzonych na zewnątrz komputera: min. 2 z przodu obudowy i 6 z tyłu. 3. Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika), PXE 2.1; 4. 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 pamięci RAM, 5. Klawiatura USB w układzie polski programisty 6. Mysz laserowa USB z rolką (scroll) 7. Nagrywarka DVD +/-RW wraz z oprogramowaniem do nagrywania i odtwarzania płyt 8. Dołączony nośnik ze sterownikami 9. Zamawiający zastrzega sobie prawo otwarcia obudów komputerów celem weryfikacji ich zgodności z zapisami umowy

2. Zasilacze awaryjne (UPS): 42 szt.

Lp.	***Nazwa komponentu***	***Wymagane minimalne parametry techniczne sprzętu***
1.	Zasilacz awaryjny (UPS)	1. typowy czas podtrzymania przy obciążeniu 50%: min. 18 minut (105 W); 2. moc wyjściowa 210W/350VA 3. napięcie wejściowe 230V 4. czas przełączania max 5ms. 5. gniazda wyjściowe 4 szt.;

		6. port komunikacji: USB
2.	Gwarancja	36-miesięczna gwarancja producenta świadczona na miejscu u klienta. Czas reakcji serwisu - do końca następnego dnia roboczego od dnia zgłoszenia usterki. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.

3. Monitory: 41 szt.

Lp.	***Nazwa komponentu***	***Wymagane minimalne parametry techniczne sprzętu***
1.	Typ ekranu	Ekran ciekłokrystaliczny z aktywną matrycą o przekątnej min. 24” format 16:9
2.	Jasność	min. 250 cd/m2
3.	Kontrast	min. 1000:1
4.	Czas reakcji matrycy	max 5ms (od czerni do bieli)
5.	Rozdzielczość	1920x1080
6.	Powłoka powierzchni ekranu	Antyodblaskowa
7.	Złącze	15-stykowe złącze D-Sub, złącze DVI-D,
8.	Gwarancja	60-miesięczna gwarancja producenta świadczona na miejscu u klienta. Czas reakcji serwisu - do końca następnego dnia roboczego od dnia zgłoszenia usterki. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.
9.	Certyfikaty	TCO 05, Energy Star 5.0
10.	Inne	Monitor musi być wyposażony w głośniki stereo.

4. Serwer sieciowy: 1 szt.

Lp.	***Nazwa komponentu***	***Wymagane minimalne parametry techniczne sprzętu***
1.	Obudowa	Typu wolnostojącego
2.	Zastosowanie	Będzie pełnił funkcję kontrolera domeny.
3.	Wydajność obliczeniowa	Komputer powinien osiągać w teście wydajności PassMark Performance Test 7.0 CPU Mark wynik min. 6900 punktów.

		W dniu dostawy Zamawiający przeprowadzi test wydajności w celu weryfikacji zgodności dostarczonego sprzętu z zamówieniem. Wyniki testów będą wydrukowane i potwierdzone przez obie strony.
4.	Pamięć operacyjna	4GB, płyta główna musi obsługiwać minimum 32GB pamięci RAM
5.	Zabezpieczenie pamięci operacyjnej	ECC lub równoważne
6.	Gniazda PCI	Minimum: 1 x PCI-Express x16 (pełnej długości) 1 x PCI-Express x8 1 x PCI-Express x4 1 x PCI-Express x1
7.	Interfejsy sieciowe	Zintegrowane 1 x 10/100/1000
8.	Napęd Optyczny	DVD+/-RW
9.	Klawiatura i mysz	USB
10.	Monitor	Typu LCD, przekątna minimalna 19'', rozdzielczość minimalna 1280x1024, spełniający normy TCO03
11.	Porty	Minimum 8 portów USB z czego minimum 2 na przednim panelu obudowy, cztery na tylnym panelu obudowy i minimum 2 porty wewnętrzne, 1x RS 232, 1 x E-SATA
12.	Dyski twarde	2 x 500GB typu SATA skonfigurowane w programowy RAID 1
14.	Wnęki na napędy	2 x wnęka 5.25"
15.	System operacyjny	Zainstalowany system Windows Server 2008 R2 Foundation w wersji 64 bitowej, posiadający polskojęzyczne wsparcie producenta sprzętu lub system równoważny.
16.	Grafika	Zintegrowana karta graficzna, lub w slocie PCI Express na kartę graficzną.
17.	Warunki gwarancji dla serwera	60-miesięczna gwarancja producenta świadczona na miejscu u klienta. Czas reakcji serwisu - do końca następnego dnia roboczego od dnia zgłoszenia usterki. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – **(załączyć do oferty dokument potwierdzający spełnianie wymogu).** Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.
18.	Certyfikaty i standardy	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 i ISO-14001 **(załączyć do oferty dokument potwierdzający spełnianie wymogu)** Deklaracja zgodności CE **(załączyć do oferty dokument potwierdzający spełnianie wymogu)** Oferowany model serwera musi znajdować się na liście Windows

		Server Catalog of Tested Products i posiadać status Certified for Windows dla systemu Windows Server 2008 R2 x64 **(załączyć do oferty dokument potwierdzający spełnianie wymogu)**
19.	Inne	Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu serwera.

5. Przełącznik sieciowy (switch): 1 szt.

Lp.	*Nazwa komponentu*	*Wymagane minimalne parametry techniczne sprzętu*
1.	Ilość portów	48 portów 10/100 /1000 BASE-T Ethernet, 4 sloty SFP umożliwiające instalację modułów 1000 BASE-SX i 1000 BASE-LX
2.	Wymiar	19 cali – do montażu w szafie rakowej, wysokość max 1 U
3.	Właściwości	• Zaawansowana diagnostyka VCD • Auto negocjacja prędkości • Automatyczne ustawianie trybu (duplex mode) • Agregacja linków (min. 4 grup 4 portowych) • Port mirroring (min. 4 portów) • Obsługa 8000 MAC adresów • Forwarding Rate 71,4 Mpps • Switching fabric 96 Gbps • Wspacie dla VLAN (64 sieci), GVRP • Wsparcie Jumbo Frames • Wsparcie Vlan trunking • Wsparcie Rapid Spanning Tree • Mozliwość działania jako DHCP server • Obsługa QoS (4 kolejki), wsparcie protokołu WRR • Obsługa Ipv6
4.	Obsługiwane standardy	• IEEE 802.3ac • IEEE 802.3ad • IEEE 802.1W • IEEE 802.1D • IEEE 802.1Q • IEEE 802.1v • IEEE 802.1p • IEEE 802.1X • IEEE 802.3x • RFC 826 • RFC 854 • RFC 855 • RFC 1155 • RFC 1157 • RFC 1213 • RFC 2579 • RFC 2580

		• RFC 2819 • RFC 3164 • RFC 3416 • RFC 768 • RFC 783 • RFC 791 • RFC 792 • RFC 793 • RFC 951 • RFC 1533 – including 1534, • RFC 2131 • RFC 2132 • RFC 950 • RFC 1123 • RFC 1042 • RFC 1071 • IGMPv2 snooping • GARP • GVRP - Dynamic VLAN Registration • GMP Snooping • Jumbo Frames • IPv6 Classification APIs
5.	Zarządzanie, zabezpieczenia	Zabezpieczenie dostępu do switcha hasłem, oraz możliwość zastrzeżenia adresów IP mających dostęp do zarządzania switchem. Interfejsy zarządzania: Telnet, CLI, SNMP V1/2, Web.
6.	Warunki gwarancji dla switcha	60-miesięczna gwarancja producenta świadczona na miejscu u klienta. Czas reakcji serwisu - do końca następnego dnia roboczego od dnia zgłoszenia usterki. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).

6. Drukarka laserowa wielofunkcyjna (sieciowa): 1 szt.

Lp.	***Nazwa komponentu***	***Wymagane minimalne parametry techniczne sprzętu***
1.	Technologia druku	technologia laserowa
2.	Format oryginału	A4
3.	Format kopii	A4-A6
4.	Prędkość druku	28 stron A4 / min.
5.	Rozdzielczość drukowania	1200x1200 dpi
6.	Czas wydruku pierwszej	maks. 6 sek.

	strony	
7.	Czas nagrzewania	maks. 20 sek. od włączenia zasilania
8.	Pobór mocy w czasie drukowania	maks. 500 W
9.	Kopiowanie wielokrotne	1- 999 kopii
10.	Pamięć RAM	min. 256 MB
11.	Zoom	25-400%
12.	Panel operatora	wyposażony w ekran LCD, opisy na panelu oraz komunikaty na ekranie w języku polskim
13.	Dupleks	w standardzie
14.	Podajnik dokumentów	automatyczny – dwustronny na min. 50 ark.
15.	Automatyczne podajniki papieru	min. 1 uniwersalna kaseta na 250 ark. A5-A4, 80 g/m2
16.	Podajnik ręczny	na min. 50 ark. A6-A4, 60-220 g/m2
17.	Funkcja druku sieciowego	w standardzie
18.	Emulacje	PCL 6, PostScript 3, XPS
19.	Interfejsy	USB 2.0, Ethernet 10/100Base-TX
20.	Funkcja skanowania sieciowego	w standardzie, skanowanie pełno-kolorowe
21.	Funkcje skanowania	skanowanie do e-mail, do FTP, do-SMB, TWAIN, WSD
22.	Rozdzielczość skanowania	min. w zakresie 200 dpi do 600 dpi
23.	Prędkość skanowania	Mono: min. 30 str./min., kolor: min. 12 str. / min. (300 dpi/A4)
24.	Typy plików	PDF, JPEG, TIFF
25.	Możliwość rozbudowy	Podajnik/podajniki papieru na min. 500 ark. formatu A4 – A5
26.	Materiały eksploatacyjne jako wyposażenie standardowe (dostarczone w komplecie w ramach oferowanej ceny jednostkowej).	Właściwa ilość tonerów, która zapewni wydrukowanie minimum 10 000 stron A4 przy 6% zaczernieniu strony. Właściwa ilość bębnów , która zapewni wydrukowanie minimum 100.000 stron A4 . Tonery i bębny muszą być nowe i nieużywane, pierwszej kategorii oraz wyprodukowane przez producenta oferowanych urządzeń.
27.	Gwarancja	36-miesięczna gwarancja producenta świadczona na miejscu u klienta. Czas reakcji serwisu - trzy dni robocze od dnia zgłoszenia usterki.

		Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.
28.	Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w wersji drukowanej w języku polskim.

7. Oprogramowanie zabezpieczające – system antywirusowy na 41 stacji roboczych + 1 serwer

Lp.	*Nazwa komponentu*	*Wymagane minimalne cechy oprogramowania*
1.	Wymagania ogólne	1. Pełne wsparcie dla systemu Windows 2000/2003/XP/PC Tablet/Vista/ Windows 2008/ Windows 7. 2. Wsparcie dla Windows Security Center (Windows XP SP2). 3. Wsparcie dla 32- i 64-bitowej wersji systemu Windows. 4. Wersja programu dla stacji roboczych Windows dostępna w języku polskim. 5. Pomoc w programie (help) w języku polskim. 6. Dokumentacja do programu dostępna w języku polskim. 7. Skuteczność programu potwierdzona nagrodami VB100 i co najmniej dwie inne niezależne organizacje np. ICSA labs lub Check Mark.
2.	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 skrótu 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 same. 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 jakiejś aktualizacji – poinformować o tym użytkownika waz 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 wyłączenia 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 rezerwowy 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, antyspam). 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. Możliwość współpracy z minimum dwoma niezależnymi serwerami centralnej administracji w taki sposób że oprogramowanie łączy się do głównego serwera i w przypadku niepowodzenia automatycznie nawiązuje połączenie z serwerem zapasowym. 67. Zarówno dla głównego serwera zarządzającego jak i dla zapasowego, administrator powinien mieć możliwość zdefiniowania niezależnie adresu IP lub nazwy hosta, portu na którym pracuje serwer oraz hasła do autoryzacji w tym serwerze.
3.	Ochrona przed spamem	1. Ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail, Windows Live Mail oraz Mozilla Thunderbird wykorzystująca filtry Bayes-a, białą i czarną listę oraz bazę charakterystyk wiadomości spamowych. 2. Program powinien umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej. 3. Pełna integracja z programami pocztowymi MS Outlook, Outlook Express, Windows Mail, Windows Live Mail oraz Mozilla Thunderbird – antyspamowe funkcje programu dostępne są bezpośrednio z paska menu programu pocztowego. 4. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego. 5. 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 z programem pocztowym. 6. Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam 7. Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam 8. Program powinien umożliwiać współpracę w swojej domyślnej konfiguracji z folderem „Wiadomości śmieci” obecnym w programie Microsoft Outlook. 9. Program powinien umożliwiać funkcjonalność która po zmianie klasyfikacji wiadomości typu spam na pożądaną zmieni jej właściwość jako „nieprzeczytana” oraz w momencie zaklasyfikowania wiadomości jako spam na automatyczne ustawienie jej właściwości jako „przeczytana”.
4.	Zapora osobista	1. Zapora osobista mogąca pracować jednym z 5 trybów: - tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko

	(personal firewall)	na znane, bezpieczne połączenia wychodzące, - tryb automatyczny z wyjątkami - działa podobnie jak tryb automatyczny, ale umożliwia administratorowi zdefiniowanie wyjątków dla ruchu przychodzącego i wychodzącego w liście reguł - tryb interaktywny – program pyta się o każde nowe nawiązywane połączenie i automatycznie tworzy dla niego regułę (na stałe lub tymczasowo) - tryb oparty na regułach – użytkownik/administrator musi ręcznie zdefiniować reguły określające jaki ruch jest blokowany a jaki przepuszczany - tryb uczenia się – umożliwia zdefiniowanie przez administratora określonego okresu czasu w którym oprogramowanie samo tworzy odpowiednie reguły zapory analizując aktywność sieciową danej stacji 2. Możliwość tworzenia list sieci zaufanych. 3. Możliwość dezaktywacji funkcji zapory sieciowej na kilka sposobów: pełna dezaktywacja wszystkich funkcji analizy ruchu sieciowego, tylko skanowanie chronionych protokołów oraz dezaktywacja do czasu ponownego uruchomienia komputera. 4. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokółu, aplikacji i adresu komputera zdalnego. 5. Możliwość wyboru jednej z 3 akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj o decyzję. 6. Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń. 7. Możliwość zapisywania w dzienniku zdarzeń związanych z zezwoleniem lub zablokowaniem danego typu ruchu. 8. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet. 9. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 10. Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu. 11. Podczas tworzenia reguł, program powinien oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6. 12. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. 13. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci 14. Administrator ma możliwość sprecyzowania, który profil zapory powinien zostać zaaplikowany po wykryciu danej sieci 15. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora 16. Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowaniu sieci bezprzewodowej lub jego braku, aktywności połączenia bezprzewodowego lub jego braku, aktywności wyłącznie jednego połączenia sieciowego lub wielu połączeń sieciowych konkretny interfejs sieciowy w systemie 17. Podczas konfiguracji autoryzacji sieci, administrator powinien mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS zarówno z wykorzystaniem adresów IPv4 jak i IPv6 18. Opcje związane z autoryzacją stref powinny oferować opcje łączenia (np. lokalny adres IP i adres serwera DNS) w dowolnej kombinacji celem zwiększenia dokładności identyfikacji danej sieci 19. Możliwość aktualizacji sterowników zapory osobistej po restarcie komputera
5.	Oprogramowanie	1. Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów plikowych Windows.

	zarządzające klientami antywirusowymi	2. Zdalna instalacja wszystkich wersji programów na stacjach roboczych i serwerach Windows NT 4.0 sp6/ 2000/XP Professional/PC Tablet/2003/ Vista/Windows 7/ 2008. 3. Do instalacji zdalnej i zarządzania zdalnego nie jest wymagany dodatkowy agent. Na końcówkach zainstalowany jest sam program antywirusowy 4. Komunikacja miedzy serwerem a klientami może być zabezpieczona hasłem. 5. 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 6. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych z opcją wygenerowania raportu ze skanowania i przesłania do konsoli zarządzającej. 7. 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). 8. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, adresów MAC, wersji systemu operacyjnego oraz domeny, do której dana stacja robocza należy. 9. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu. 10. Możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych. 11. Możliwość tworzenia grup stacji roboczych i definiowania w ramach grupy wspólnych ustawień konfiguracyjnymi dla zarządzanych programów. 12. Możliwość importowania konfiguracji programu z wybranej stacji roboczej/serwera a następnie przesłanie (skopiowanie) jej na inną stację/ serwer lub grupę stacji roboczych w sieci. 13. 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). 14. Możliwość uruchomienia serwera zdalnej administracji na stacjach Windows NT4 (Service Pack 6)/2000/XP/Vista/Windows 7 oraz na serwerach Windows NT 4.0 sp6/2000/2003/2008 – 32 i 64-bitowe systemy. 15. Możliwość uruchomienia centralnej konsoli zarządzającej na stacji roboczej Windows 2000/XP/Vista/Windows 7, oraz na serwerach Windows 2000/2003/2008 - 32 i 64-bitowe systemy. 16. Możliwość wymuszenia konieczności uwierzytelniania stacji roboczych przed połączeniem się z serwerem zarządzającym. Uwierzytelnianie przy pomocy zdefiniowanego na serwerze hasła. 17. 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 w pełni kompatybilną z formatem bazy danych programu Microsoft Access. 18. Serwer centralnej administracji powinien oferować administratorowi możliwość współpracy przynajmniej z trzema zewnętrznymi motorami baz danych w tym minimum z: Microsoft SQL Server, MySQL Server oraz Oracle. 19. Do instalacji serwera centralnej administracji nie jest wymagane zainstalowanie dodatkowych aplikacji takich jak Internet Information Service (IIS) czy Apache. 20. Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) w formacie HTML lub CSV. 21. 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). 22. Serwer centralnej administracji powinien oferować funkcjonalność synchronizacji grup komputerów z drzewem Active Directory. Synchronizacja

		ta, powinna automatycznie umieszczać komputery należące do zadanych grup w AD do odpowiadających im grup w programie. Funkcjonalność ta nie powinna wymagać instalacji serwera centralnej administracji na komputerze pełniącym funkcję kontrolera domeny. 23. Serwer centralnej administracji powinien umożliwiać definiowanie różnych kryteriów wobec podłączonych do niego klientów (w tym minimum przynależność do grupy roboczej, przynależność do domeny, adres IP, adres sieci/podsieci, zakres adresów IP, nazwa hosta, przynależność do grupy, brak przynależności do grupy). Po spełnieniu zadanego kryterium lub kilku z nich stacja powinna otrzymać odpowiednią konfigurację. 24. Serwer centralnej administracji powinien być wyposażony w mechanizm informowania administratora o wykryciu nieprawidłowości w funkcjonowaniu oprogramowania zainstalowanego na klientach w tym przynajmniej informowaniu o: wygaśnięciu licencji na oprogramowanie, o tym że zdefiniowany procent z pośród wszystkich stacji podłączonych do serwera ma nieaktywną ochronę oraz że niektórzy z klientów podłączonych do serwera oczekują na ponowne uruchomienie po aktualizacji do nowej wersji oprogramowania. 25. Serwer centralnej administracji powinien być wyposażony w wygodny mechanizm zarządzania licencjami, który umożliwi sumowanie liczby licencji nabytych przez użytkownika. Dodatkowo serwer powinien informować o tym, ilu stanowiskową licencję posiada użytkownik i stale nadzorować ile licencji spośród puli nie zostało jeszcze wykorzystanych. 26. W sytuacji, gdy użytkownik wykorzysta wszystkie licencje, które posiada po zakupie oprogramowania, administrator po zalogowaniu się do serwera poprzez konsolę administracyjną powinien zostać poinformowany o tym fakcie za pomocą okna informacyjnego. 27. Możliwość tworzenia repozytorium aktualizacji na serwerze centralnego zarządzania i udostępniania go przez wbudowany serwer http. 28. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. 29. Dostęp do kwarantanny klienta z poziomu systemu zdalnego zarządzania. 30. Możliwość przywrócenia lub pobrania zainfekowanego pliku ze stacji klienckiej przy wykorzystaniu zdalnej administracji 31. Administrator powinien mieć możliwość przywrócenia i wyłączenia ze skanowania pliku pobranego z kwarantanny stacji klienckiej 32. Podczas przywracania pliku, administrator powinien mieć możliwość zdefiniowania kryteriów dla plików które zostaną przywrócone w tym minimum: zakres czasu z dokładnością co do minuty kiedy wykryto daną infekcję, nazwa danego zagrożenia, dokładna nazwa wykrytego obiektu oraz zakres minimalnej i maksymalnej wielkości pliku z dokładnością do jednego bajta. 33. Kreator konfiguracji zapory osobistej stacji klienckich pracujących w sieci, umożliwiający podgląd i utworzenie globalnych reguł w oparciu o reguły odczytane ze wszystkich lub z wybranych komputerów lub ich grup. 34. Możliwość utworzenia grup do których przynależność jest aplikowana dynamicznie na podstawie zmieniających się parametrów klientów w tym minimum w oparciu o: wersję bazy sygnatur wirusów, maskę wersji bazy sygnatur wirusów, nazwę zainstalowanej aplikacji, dokładną wersję zainstalowanej aplikacji, przynależność do domeny lub grupy roboczej, przynależność do serwera zdalnego zarządzania, przynależności lub jej braku do grup statycznych, nazwę komputera lub jej maskę, adres IP, zakres adresów IP, przypisaną politykę, czas ostatniego połączenia z systemem centralnej administracji, oczekiwania na restart, ostatnie zdarzenie związane z wirusem, ostatnie zdarzenie związane z zaporą i systemem IDS, ostatnie zdarzenie związane z usługą programu lub jego procesem, ostatnie zdarzenie związane ze skanowaniem na żądanie oraz z nieudanym leczeniem podczas takiego skanowania, maską wersji systemu operacyjnego oraz flagą klienta mobilnego.

		35. Podczas tworzenia grup dynamicznych, parametry dla klientów można dowolnie łączyć oraz dokonywać wykluczeń pomiędzy nimi. 36. Utworzone grupy dynamiczne mogą współpracować z grupami statycznymi.

8. Oprogramowanie zabezpieczające – kontrola rodzicielska na 42 stacje robocze

Lp.	***Nazwa komponentu***	***Wymagane minimalne cechy oprogramowania***
1.	Oprogramowanie zabezpieczające (kontrola rodzicielska)	1. Oprogramowanie przeznaczone dla systemów operacyjnych: Windows 2000, XP, Vista oraz Windows 7 (32 oraz 64 bit) 2. Blokada dostępu do stron o tematyce erotycznej: Domyślnie włączona. Powoduje zablokowanie dostępu do stron zawierających treści erotyczne. 3. Możliwość ustalenia adresów stron internetowych, które będą całkowicie zablokowane. 4. Możliwość kontroli dostępu do komunikatorów i serwisów wideo, portali społecznościowych 5. Możliwość przeglądania historii przeglądanych stron internetowych 6. Możliwość ustalenia adresów stron internetowych, do których użytkownik będzie miał dostęp, a pozostałe będą zablokowane. 7. Możliwość blokady pobierania z Internetu plików wykonywalnych np. EXE 8. Możliwość blokady pobierania z Internetu plików dokumentów np. plików z rozszerzeniami DOC, XLS, ZIP itd. 9. Możliwość blokowania funkcji systemu Windows „Nagraj płytę CD” 10. Możliwość blokowania funkcji zapisu na pamięciach przenośnych USB 11. Możliwość blokowania dostępu do Panelu Sterowania 12. Możliwość blokowania dostępu do „Dodaj/Usuń programy” z Panelu Sterowania 13. Możliwość blokowania funkcji „Uruchom” z menu Start 14. Możliwość blokady dostępu do list dyskusyjnych (NNTP) poprzez blokadę portu. 15. Możliwość blokady dostępu do emaili (POP3 i SMTP) poprzez blokadę portów. 16. Możliwości określenia ograniczeń czasowych do przeglądania stron internetowych tj. ograniczenie dziennego czasu dostępu do Internetu, określenie przedziału czasu dla każdego dnia tygodnia osobno. 17. Możliwość ustawienia zapisywania widoku pulpitu systemu z określoną częstotliwością min.30 sek – max. 10 min. oraz określenia co ile dni zapisane widoki mają być usuwane 18. Możliwość blokady dostępu do konfiguracji oprogramowania za pomocą hasła. 19. Wersja programu dla stacji roboczych Windows dostępna w języku polskim.