

Wymagane i oferowane parametry jakościowe i techniczne – Kompletne stanowisko komputerowe PC

KOMPLETNE ZESTAWY KOMPUTEROWE - 6 kompletów (jednostka centralna – stacjonarna +monitor LCD+ oprogramowanie systemowe +pakiet antywirusowy)		
	Minimalne parametry wymagane	Parametry oferowane (Wypełnia <u>dokładnie</u> Wykonawca)
Typ	komputer stacjonarny typu MiniTower	
Zastosowanie	praca z zainstalowaną medyczną aplikacją bazodanową	
Wydajność obliczeniowa	w testach aplikacyjnych SYSmark 2012 Rating zestaw powinien osiągać wynik minimum 130 punktów	
Pamięć operacyjna	minimum 4 GB	
	pozostają wolne 1 sloty na rozszerzenie	
	maksymalna obsługa 8GB	
Wydajność grafiki	zestaw powinien poprawnie pracować z rozdzielczością HD	
Monitor	typ wyświetlacza: TFT-TN	
	obszar aktywny: 20cali	
	kontrast: 2 000 000 (dynamiczny) : 1, 1 000 : 1 (typowy)	
	jasność: 250 cd/m2	
	czas reakcji: 5ms	
	rozdzielczość podstawowa: 1600x900	
	certyfikaty i standardy: TCO 5.0, Eergy Star 5.0, EPEAT Gold	
	złącza: DSub (analogowe) i DVI ZHDCP (cyfrowe)	
	Monitor musi pochodzić od tego samego producenta co zestaw komputerowy	
Pamięć masowa	HDD, minimum 500GB, SATA 3	
	Napęd DVD+/- RW Dual Layer	
Zgodność z systemami operacyjnymi i standardami	Potwierdzona certyfikatem WHQL oraz certyfikatem CE	
Ergonomia	głośność przy maksymalnym obciążeniu nie może przekraczać 40dB	

Warunki gwarancji	minimum 3 lata na całość od momentu podpisania protokołu odbioru	
	w przypadku awarii i konieczności zabrania jednostki centralnej z siedziby Zamawiającego pamięć masowa (dyski) pozostaje u Zamawiającego	
	czas usunięcia uszkodzenia 14 dni roboczych od momentu zgłoszenia awarii, sprzęt do naprawy i z naprawy Wykonawca dostarcza na swój koszt, w przypadku niemożności naprawy w ww. terminie - dostarczenie sprzętu zastępczego o nie gorszych parametrach techniczno-użytkowych	
	w przypadku uszkodzenia pamięci masowej (dysków) - uszkodzona pozostaje własnością Zamawiającego	
	serwis sprzętu musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta	
Wsparcie techniczne	dostępność wszystkich sterowników koniecznych do prawidłowej pracy zestawu poprzez witrynę producenta zestawu komputerowego	
Wymagania dodatkowe	na etapie składania oferty Wykonawca zobowiązany jest przedstawić dokładną specyfikację zaproponowanych podzespołów, które będą wykorzystane w zaoferowanym zestawie komputerowym	
	nie dopuszcza się stosowania tzw. overclockingu w celu uzyskania wymaganych parametrów pracy zestawu komputerowego	
	zainstalowany system operacyjny wg wymagań wyszczególnionych w tabeli poniżej wraz z nośnikiem instalacyjnym na płycie DVD i licencją dożywotnią	
	dołączony pakiet oprogramowania antywirusowego z firewallem wg wyszczególnionych w tabeli poniżej	
	kolorystyka obudowy czarna, wielkość mini tower, wysokość nie przekraczająca 360mm, szerokość do 180mm, ilość kieszeni wewnętrznych 3.5" minimum 1, z przodu obudowy wyjścia audio i USB, wyjście HDMI	
	klawiatura czarna 104 klawisze w układzie polski programisty na złączu USB, mysz czarna optyczna z kółkiem na złączu USB i rozdzielczości minimum 800dpi	
	możliwość w biosie płyty głównej wyłączenie wszystkich portów USB	
	możliwość załączenia funkcji WOL dla karty sieciowej	
	pamięć operacyjna o przepustowości 16000 MB/s, markowe, z radiatorem chłodzącym	
	płyta główna ma być wyposażona w zintegrowaną kartę graficzną umożliwiającą pracę na minimum 2 monitorach jednocześnie, gigabitową kartę sieciową, w standardzie micro-atx, zasilacz z aktywnym PFC	
	procesor o zużyciu prądu max 65W	
	wymagana jest jednolita pula komponentów dla wszystkich zamawianych zestawów komputerowych	

Oświadczam, że oferowany przedmiot zamówienia spełnia wszystkie wymienione w powyższej tabeli wymagania:

.....

SYSTEM OPERACYJNY	
1. Wymagania dla systemu operacyjnego 32/64-bit:	Tak / Nie
a) nie wymaga aktywacji za pomocą telefonu lub Internetu u producenta	
b) dołączony nośnik z oprogramowaniem	
c) licencja dożywotnia użytkownika	
d) poprawna obsługa pamięć operacyjnej w ilości powyżej 4GB	
2. System musi spełniać następujące wymagania poprzez natywne dla niego mechanizmy, bez użycia dodatkowych aplikacji:	Tak / Nie
a) możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek; możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu; darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat); internetowa aktualizacja zapewniona w języku polskim; wbudowana zaporę internetową (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IPv4 i IPv6; zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimedialny, pomoc, komunikaty systemowe; wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi); funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer; interfejs użytkownika działający w trybie graficznym z elementami 3D; zintegrowana z interfejsem użytkownika interaktywna część pulpitu służąca do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta; możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu; zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników; zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych; zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych; funkcje związane z obsługą komputerów typu TABLET PC, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego; funkcjonalność rozpoznawania mowy, pozwalająca na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika; zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi; wbudowany system pomocy w języku polskim; możliwość przystosowania stanowiska dla osób niepełnosprawnych (i słabo widzących);	
b) możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji; wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509; wsparcie dla logowania przy pomocy smartcard; rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji; system posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; wsparcie dla Sun Java i .NET Framework 1.1, 2.0, 3.0 i 4.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach; wsparcie dla Jscript i VBScript – możliwość uruchamiania interpretera poleceń; zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem; rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami (obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową); rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację; graficzne środowisko instalacji i konfiguracji; transakcyjny system plików pozwalający na stosowanie przydziałów na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe; zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe; udostępnianie modemu; oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej; możliwość przywracania plików systemowych; system operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.); możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (i przy użyciu numerów identyfikacyjnych sprzętu);	

3. Współpraca z posiadanymi aplikacjami:		Tak / Nie
a)	ze względu na posiadane przez Zamawiającego oprogramowanie Microsoft Office 2003/2007/2010 wymagana jest możliwość instalacji tego oprogramowania na systemie operacyjnym oferowanym przez Wykonawcę	
b)	ze względu na posiadaną przez Zamawiającego aplikację bazodanową InfoMedica (firmy Asseco Poland S.A.) wymagana jest możliwość instalacji tego oprogramowania na systemie operacyjnym oferowanym przez Wykonawcę	
c)	zaoferowany system operacyjny będzie mógł być wykorzystywany (bez konieczności wykonywania jakichkolwiek modyfikacji) w sieciach informatycznych do przetwarzania informacji wrażliwych (dane osobowe, dane medyczne, dane finansowe)	

PAKIET ANTYWIRUSOWY		
Wymagania dla pakietu antywirusowego		Tak / Nie
Zamawiający oświadcza, iż obecnie posiada 228 licencji pakietu antywirusowego ESET Smart Security Business Edition na okres od 29.05.2012 do 28.05.2014 wraz z wdrożoną konsolą do centralnego zarządzania		---
W przypadku zaoferowania ESET Smart Security Business Edition/ ESET Endpoint Security Zamawiający nie wymaga wdrożenia i uruchomienia konsoli centralnego zarządzania		---
1. Pakiet oprogramowania antywirusowego musi posiadać:		---
a)	wersja oprogramowania - polskojęzyczna w całości	
b)	licencja na okres 1 roku kalendarzowego (365 dni) od dnia dostarczenia Zamawiającemu	
c)	licencja zbiorcza na 20 stanowisk (jeden klucz)	
d)	konsola centralnego zarządzania	
2. Oferowany pakiet antywirusowy:		---
ESET Smart Security Business Edition/ ESET Endpoint Security:		
Wymagania dla rozwiązania równoważnego (podać nazwę i wersję oferowanego rozwiązania poniżej):		---
.....		
.....		
		Tak / Nie
a)	licencje na oprogramowanie antywirusowe wraz z firewallem	
b)	konsola wraz z wdrożeniem do centralnego zarządzania oprogramowaniem (w przypadku zaoferowania oprogramowania innego niż posiadane dotychczas przez Zamawiającego)	
c)	stacje robocze: pełne wsparcie dla systemu Windows 2000/2003/2008/XP/Vista/7, Windows Security Center (Windows XP SP2); Wsparcie dla 32- i 64-bitowej wersji systemu Windows; Interfejs programu, pomoc w programie oraz dokumentacja do programu dostępne w języku polskim; skuteczność programu potwierdzona nagrodami VB100 i co najmniej dwie inne niezależne organizacje np. ICSA labs lub Check Mark; wydajność wg testów z października 2012 przeprowadzonego przez niezależną organizację AntiVirus-Comparative na poziomie minimum 187,7 punktów (http://www.av-comparatives.org/images/stories/t/performance/avc_per_201210_en.pdf) oraz zaklasyfikowany na poziomie Advanced+.	

- d) Ochrona antywirusowa i antyspyware: pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami; wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.; wbudowana technologia do ochrony przed rootkitami; skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików; możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu; możliwość utworzenia wielu różnych zadań skanowania według harmonogramu; skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym; możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania; możliwość skanowania dysków sieciowych i dysków przenośnych; skanowanie plików spakowanych i skompresowanych; możliwość definiowania listy rozszerzeń plików, które mają być skanowane; możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach; możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny); skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy powszechnie używanych programów pocztowych; skanowanie i oczyszczanie poczty przychodzącej POP3 "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego); automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji; możliwość definiowania różnych portów dla POP3, na których ma odbywać się skanowanie; możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail; skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie; blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występujące w nawie strony; automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji; wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka); możliwość automatycznego wysyłania powiadomienia o wykrytych zagrożeniach do dowolnej stacji roboczej w sieci lokalnej; w przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e mail; możliwość zabezpieczenia hasłem dostępu do opcji konfiguracyjnych programu; możliwość zabezpieczenia hasłem możliwości wyłączenia programu antywirusowego i poszczególnych funkcji programu; automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń; aktualizacja dostępna bezpośrednio z Internetu, z lokalnego zasobu sieciowego; obsługa pobierania aktualizacji za pośrednictwem serwera proxy; możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja); do każdego zadania aktualizacji można przypisać dwa różne profile z innym ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja); 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; praca programu musi być niezauważalna dla użytkownika; program powinien posiadać dwa interfejsy programu (standardowy i dla zaawansowanych użytkowników); dziennik zdarzeń rejestrujący informacje na temat znalezionych C1C1zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania;
- e) Ochrona przed spamem: ochrona antyspamowa dla programów pocztowych wykorzystująca filtry Bayes a, białą i czarną listę oraz bazę charakterystyk wiadomości spamowych; program powinien umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej; pełna integracja z powszechnie używanymi programami pocztowymi, Windows Live Mail – antyspamowe funkcje programu dostępne są bezpośrednio z paska menu programu pocztowego; automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego; możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną wiadomość i odwrotnie oraz ręcznego dodania wiadomości do białej i czarnej listy z wykorzystaniem funkcji programu zintegrowanych z programem pocztowym; możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam; możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam; program powinien umożliwiać współpracę w swojej domyślnej konfiguracji z folderem „Wiadomości śmieci” obecnym w programie pocztowym; 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”;

f)	<p>Zapora osobista (personal firewall): zapora osobista mogąca pracować w jednym z podanych trybów: - 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; możliwość tworzenia list sieci zaufanych; 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; możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego; możliwość wyboru jednej z 3 akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj o decyzję; możliwość zdefiniowania 2 oddzielnych zestawów reguł – jeden dla strefy zaufanej (sieć wewnętrzna) i drugi niezaufanej (Internet); wbudowany system IDS; wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu; wsparcie techniczne do programu świadczone w języku polskim przez polskiego autoryzowanego dystrybutora;</p>
g)	<p>Konsola zdalnej administracji: centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów Windows; zdalna instalacja wszystkich wersji programów na stacjach roboczych i serwerach Windows 2000/2003/2008/XP/Vista/7; centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, oraz zaporą osobistą (tworzenie reguł obowiązujących dla wszystkich stacji) zainstalowanymi na stacjach roboczych w sieci z jednego serwera zarządzającego; możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych z wygenerowaniem raportu ze skanowania i przesłaniem do konsoli zarządzającej; możliwość sprawdzania stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie i skanerów rezydentnych); możliwość sprawdzania podstawowych informacji dotyczących stacji roboczej: adresów IP, adresów MAC, wersji systemu operacyjnego oraz domeny, do której dana stacja robocza należy; możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu; możliwość skanowania sieci w poszukiwaniu niezabezpieczonych stacji roboczych; możliwość tworzenia grup stacji roboczych i definiowania w ramach grupy wspólnych ustawień konfiguracyjnymi dla zarządzanych programów; możliwość zmiany konfiguracji na stacjach i serwerach; możliwość instalacji na stacjach z systemem operacyjnym Windows 2000/2003/2008/XP/Vista - 32 i 64-bitowe systemy; możliwość uruchomienia na dowolnej stacji roboczej z systemem operacyjnym Windows 2000/2003/2008/XP/Vista/7 - 32 i 64-bitowe systemy; serwer centralnej administracji powinien oferować administratorowi możliwość współpracy z zewnętrznymi motorami baz danych; do instalacji nie jest wymagane zainstalowanie dodatkowych aplikacji; możliwość ręcznego (na żądanie) i automatycznego generowania raportów (według ustalonego harmonogramu) w formacie HTML lub CSV; możliwość tworzenia hierarchicznej struktury serwerów zarządzających i replikowania informacji pomiędzy nimi w taki sposób, aby nadrzędny serwer miał wgląd w swoje stacje robocze i we wszystkie stacje robocze serwerów podrzędnych (struktura drzewiasta); możliwość 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; możliwość definiowania różnych kryteriów wobec podłączonych klientów (w tym minimum przynależność do grupy roboczej, przynależność do domeny, adres IP, adres sieci/podsieci, zakres adresów IP, nazwa hosta); mechanizm informowania administratora o wykryciu nieprawidłowości w funkcjonowaniu oprogramowania zainstalowanego na klientach; mechanizm zarządzania licencjami który umożliwi sumowanie liczby licencji nabytych przez użytkownika;</p>