Załącznik nr 1
Opis przedmiotu zamówienia

SPIS TREŚCI

1 Określenie przedmiotu zamówienia 2
1.1 Opis przedmiotu zamówienia - Projektu 2
1.2 Termin realizacji zamówienia 2
1.3 Infrastruktura sprzętowa 2
1.3.1 Zestaw do podpisów elektronicznych 2
1.3.2 Zestawy komputerowe 3
1.3.3 Komputery przenośne dla Radnych 15
1.3.4 Komputery przenośne dla kadry zarządzającej i pracowników 25
1.3.5 Zarządzalny przełącznik – Switch 37
1.3.6 Karty rozszerzeń do serwerów i Oprogramowanie 37
1.3.7 Macierz dyskowa 39
1.3.8 Laserowe urządzenie wielofunkcyjne A3 41
1.3.9 Laserowe urządzenie wielofunkcyjne A4 42
1.3.10 Drukarka kodów kreskowych współpracująca z EZD 44

1 Określenie przedmiotu zamówienia

1.1 Opis przedmiotu zamówienia - Projektu

W ramach realizacji projektu pt.: „**Zwiększenie dostępu do cyfrowych usług publicznych na terenie Gminy Kruszyna**” planowane jest:

Lp.	Przedmiot zamówienia
Dostawa sprzętu do uruchomienia e-usług	
1	Zestawy do podpisów elektronicznych
2	Zestawy komputerowe
3	Komputery przenośne dla Radnych
4	Komputery przenośne dla kadry zarządzającej i pracowników obsługi Rady Gminy
5	Zarządzalny przełącznik - Switch
6	Karty rozszerzeń oraz oprogramowanie do Serwera DELL POWEREDGE R510
7	Karty rozszerzeń oraz oprogramowanie do Serwera DELL POWEREDGE R520
8	Karty rozszerzeń oraz oprogramowanie do Serwera DELL POWEREDGE R710
9	Macierz dyskowa
10	Laserowe urządzenie wielofunkcyjne A3
11	Laserowe urządzenie wielofunkcyjne A4
12	Drukarka kodów kreskowych współpracująca z EZD

Zamawiający informuje, że w przypadku gdy określił w niniejszym dokumencie wymagania z użyciem znaków towarowych, patentów, pochodzenia, norm, aprobat, specyfikacji technicznych lub systemów odniesienia, to należy traktować takie określenie jako przykładowe. W każdym takim przypadku Zamawiający dopuszcza zaoferowanie rozwiązań równoważnych o parametrach nie gorszych niż wskazane.

1.2 Termin realizacji zamówienia

Przedmiot umowy musi być zrealizowany zgodnie ze złożoną ofertą lecz nie później niż w terminie 60 dni od dnia podpisania umowy.
Płatności będą realizowane w terminie 30 dni od daty otrzymania prawidłowo wystawionej faktury VAT. Wystawienie faktur następuje po podpisaniu przez Zamawiającego (bez uwag) Protokołu Odbioru przedmiotu zamówienia.

1.3 Infrastruktura sprzętowa

1.3.1 ZESTAW DO PODPISÓW ELEKTRONICZNYCH

Zestawy do podpisów elektronicznych – 10 szt.
Minimalne wyposażenie zestawu do podpisów elektronicznych:

- Karta kryptograficzna;

- Czytnik kart;
- Płyta z oprogramowaniem;
- Certyfikat kwalifikowany.

1.3.2 ZESTAWY KOMPUTEROWE

Komputer stacjonarny – 15 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
Typ	Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej i jako lokalna baza danych.
Wydajność obliczeniowa	Procesor dedykowany do pracy w komputerach stacjonarnych. Oferowany procesor powinien osiągać w teście wydajności Passmark CPU Mark co najmniej 10000 punktów. Dokumentem potwierdzającym spełnianie ww. wymagań będzie wydruk ze strony https://www.cpubenchmark.net/cpu_list.php. Dokumenty potwierdzające spełnienie powyższych wymagań (wydruk ze strony internetowej potwierdzający osiągnięty wynik) załączyć na wezwanie Zamawiającego zgodnie z art. 26 ust. 2 ustawy prawo zamówień publicznych.
Pamięć operacyjna RAM	8GB możliwość rozbudowy do min. 32GB min. dwa sloty wolne.
Parametry pamięci masowej	Min. 1TB
Wydajność grafiki	Grafika zintegrowana z procesorem powinna umożliwiać pracę dwumonitorową z wsparciem DirectX 12, OpenGL 5.0, OpenCL 1.2; pamięć współdzielona z pamięcią RAM, przydzielana dynamicznie, obsługująca rozdzielczości min: 3840x2160 @ 60Hz (cyfrowo) 2560x1600 @ 60Hz (cyfrowo) 1920x1200 @ 60Hz (analogowo i cyfrowo)
Wyposażenie multimedialne	Min. czterokanałowa (24-bitowa) karta dźwiękowa, zintegrowana z płytą główną, zgodna z High Definition, 3 wyjścia Audio na tylnym panelu obudowy; Porty słuchawek i mikrofonu na przednim oraz na tylnym panelu obudowy.
Obudowa	Typu MiniTower wyposażona w min. 3 kieszenie: 1 szt. 5,25” zewnętrzna pełnych wymiarów (nie dopuszcza się wnęk typu slim), 2 szt. 3,5” wewnętrzne. Obudowa powinna fabrycznie umożliwiać montaż min. 2 szt. dysku 3,5” z możliwością instalacji dysków 2,5”. Zasilacz wewnętrzny o mocy nie mniejszej niż 250W pracujący w sieci 230V 50/60Hz prądu zmiennego o sprawności min. 90%. Zasilacz spełniający wymóg 80plus. Zasilacz w oferowanym komputerze musi znajdować się na stronie internetowej http://www.plugloadsolutions.com/80pluspowersupplies.aspx Dokumenty potwierdzające spełnienie powyższego wymagania (wydruk ze strony internetowej potwierdzający spełnienie wymogu) załączyć na wezwanie Zamawiającego zgodnie z art. 26 ust. 2 ustawy prawo zamówień publicznych. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady) oraz kłódki (oczko w obudowie do założenia kłódki).

	Obudowa musi posiadać wbudowany dźwiękowy system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, a w szczególności musi sygnalizować: - uszkodzenie lub brak pamięci RAM, - uszkodzenie złączy PCI i PCIe lub płyty głównej, - uszkodzenie dysku twardego. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów wymaganych w specyfikacji. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS.
Zgodność z systemami operacyjnymi i standardami	Potwierdzenie kompatybilności komputera na daną platformę systemową zaoferowaną z komputerem. Dokumenty potwierdzające spełnienie powyższych wymagań (wydruk ze strony internetowej lub certyfikat producenta systemu operacyjnego potwierdzający spełnianie wymogu) załączyć na wezwanie Zamawiającego zgodnie z art. 26 ust. 2 ustawy prawo zamówień publicznych.
System Operacyjny	Zainstalowany system musi spełniać następujące wymagania, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: • 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 zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; • Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, 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 służącą 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.

	• Funkcjonalność rozpoznawania mowy, pozwalającą 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 (np. słabo widzących); • 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; • 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 i 2.0 i 3.0 – 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 za logowanego 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 ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację; • Graficzne środowisko instalacji i konfiguracji; • Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) 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. • 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 (np. przy użyciu numerów identyfikacyjnych sprzętu).
BIOS	• BIOS zgodny ze specyfikacją UEFI • Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: o wersji BIOS, o nr seryjnym komputera, o ilości pamięci RAM, o typie procesora, o pojemności zainstalowanego dysku twardego, o rodzajach napędów optycznych,

	o kontrolerze audio. • Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego • Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń • BIOS ma być w pełni obsługiwany przez interfejs myszy i klawiatury oraz w pełni wykorzystywać dyski twarde większe niż 2.2TB • 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 włączenia/wyłączenia zintegrowanej karty dźwiękowej, karty sieciowej, wbudowanych portów z poziomu BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. • Możliwość ustawienia portów USB w trybie „no BOOT", czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. • Możliwość wyłączania portów USB.
Certyfikaty i standardy	• Certyfikat ISO9001 lub równoważny, dla producenta sprzętu • Deklaracja zgodności CE lub równoważna • Komputer musi spełniać wymogi normy Energy Star 6.0 - wymagany wpis dotyczący oferowanego komputera w internetowym katalogu http://www.eu-energystar.org lub http://www.energystar.gov <u>Dokumenty potwierdzające spełnienie powyższych wymagań załączyć na wezwanie Zamawiającego zgodnie z art. 26 ust. 2 ustawy prawo zamówień publicznych.</u>
Warunki gwarancji	Min. 3-letnia gwarancja (trzy letnia lub dłużej zgodnie ze złożoną ofertą), świadczona na miejscu u klienta, czas reakcji serwisu - do końca następnego dnia roboczego. W przypadku awarii dysków twardych, dysk pozostaje u Zamawiającego bez ponoszenia dodatkowych kosztów.
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.
Wymagania dodatkowe	Wbudowane porty: • min. 1 x VGA, • min. 1 x DisplayPort • min. 1 x HDMI ver. 1.4 • min. 8 portów USB wyprowadzonych na zewnątrz komputera w tym min. 4xUSB 3.0: min. 2 porty z przodu obudowy w tym 1 port USB 3.0 i 1 port USB 2.0 lub 2 porty USB 3.0 i 6 portów na tylnym panelu w tym min. 2 porty USB 3.0, wymagana ilość i rozmieszczenie

	portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, kart PCIe itp. • porty słuchawek i mikrofonu na przednim oraz tylnym panelu obudowy. • Komputer musi umożliwiać jego rozbudowę w postaci dedykowanych kart PCIe np. kartę WiFi a/b/g/n • wbudowany czytnik Kart Multimedialnych min. 6-w-1 w tym: SD/ MMC/ SDHC, • wbudowany czytnik SmartCard – Czytnik kart mikroprocesorowych zgodny z ISO 7816-1,2,3,4 • Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę Jumbo Frames i Flow Control • Płyta główna jednostki wyposażona w: min. 1 wolne złącze PCI Express x16 Gen.3 min. 1 wolne złącze PCI Express x 1 • Klawiatura USB w układzie polski programisty • Mysz USB z klawiszami oraz rolką (scroll) • Nagrywarka DVD +/-RW szybkość min. x24 wraz z oprogramowaniem do nagrywania i odtwarzania płyt • Dołączony nośnik ze sterownikami • Wbudowany w płytę główną układ przetwarzania energii, zapewniający możliwość całościowego zarządzania poziomem zużywanej energii poprzez wykrywanie aktualnego poziomu wykorzystania zasobów PC (CPU, GPU, HDD, zasilacza) oraz inteligentne przydzielanie mocy w czasie rzeczywistym. Układ działający automatycznie od momentu uruchomienia komputera.
Antywirus	Istotne cechy oprogramowania: 1. Ochrona antywirusowa stacji roboczych pracujących pod kontrolą systemów operacyjnych Windows 7, 8, 8.1, 10 w wersjach 32-bit oraz 64-bit oraz dostarczonym z zaoferowanym w ramach niniejszego postępowania. 2. Ochrona antywirusowa wyżej wymienionych systemów zarządzana i monitorowana z pojedynczej, centralnej konsoli. 3. Serwer konsoli zarządzania pracujący pod kontrolą wymienionych niżej systemów: - Windows Server 2008 SP1 (32-bit) edycji Standard, Enterprise oraz Web Server - Windows Server 2008 SP1 (64-bit) edycji Standard, Enterprise, Web Server, Small Bussines Server oraz Essential Bussines Server - Windows Server 2008 R2 oraz Windows Server 2008 R2 SP1 edycji Standard, Enterprise oraz Web Server - Windows Server 2012 edycji Essentials, Standard oraz Datacenter - Windows Server 2012 R2 edycji Essentials, Standard oraz Datacenter - Windows Server 2016 edycji Essentials, Standard oraz Datacenter - Red Hat Enterprise Linux 5, 6 and 7 (32-bit oraz b4-bit) - CentOS 6, 7 (32-bit oraz b4-bit) - openSUSE 13.2 (32-bit oraz b4-bit) - SUSELinuxEnterpriseServer10 and 11 (32-bit oraz b4-bit) - SUSE Linux Enterprise Desktop 11 (32-bit oraz b4-bit) - Debian GNU Linux 7 and 8 (32-bit oraz b4-bit) - Ubuntu 12.04, 14.04, 16.04 (32-bit oraz b4-bit) 4. Konsola zarządzania pracująca pod kontrolą wymienionych niżej systemów: - Windows 7 i Windows 7 SP1 (32-bit oraz 64-bit) edycji Professional, Enterprise oraz Ultimate

	- Windows 8 (32-bit oraz 64-bit) wszystkie edycje - Windows 8.1 (32-bit oraz 64-bit) wszystkie edycje - Windows 10 (32-bit oraz 64-bit) - Windows Server 2008 SP1 (32-bit) edycji Standard, Enterprise oraz Web Server - Windows Server 2008 SP1 (64-bit) edycji Standard, Enterprise, Web Server, Small Bussines Server oraz Essential Bussines Server - Windows Server 2008 R2 oraz Windows Server 2008 R2 SP1 edycji Standard, Enterprise oraz Web Server - Windows Server 2012 edycji Essentials, Standard oraz Datacenter - Windows Server 2012 R2 edycji Essentials, Standard oraz Datacenter - Windows Server 2016 edycji Essentials, Standard oraz Datacenter - Red Hat Enterprise Linux 5, 6 and 7 (32-bit oraz 64-bit) - CentOS 6, 7 (32-bit oraz b4-bit) - openSUSE 13.2 (32-bit oraz b4-bit) - SUSE Linux Enterprise Server 10 and 11 (32-bit oraz b4-bit) - SUSE Linux Enterprise Desktop 11 (32-bit oraz b4-bit) - Debian GNU Linux 7 and 8 (32-bit oraz b4-bit) - Ubuntu 12.04, 14.04, 16.04 (32-bit oraz b4-bit) 5. Możliwość instalacji konsoli zarządzania niezależnie na kilku wybranych stacjach. 6. Polski interfejs użytkownika i dokumentacja do oprogramowania na stację roboczą. Wymagania dotyczące technologii: 1. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanującego nośniki i monitora poczty elektronicznej, monitora ruchu http oraz moduł antyrootkitowy. 2. Co najmniej trzy różne silniki antywirusowe, funkcjonujące jednocześnie i skanujące wszystkie dane. 3. Oddzielny silnik skanujący do wykrywania niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan". 4. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie. 5. Możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta. 6. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie. 7. Brak konieczności restartu komputerów po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów. 8. Heurystyczna technologia do wykrywania nowych, nieznanych wirusów. 9. Wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan", „rootkit". 10. Możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger", „dialer", „trojan" w kwarantannie. 11. Mechanizm centralnego zarządzania folderami kwarantanny znajdującymi się na stacjach klienckich. 12. Mechanizm skanujący wspólny dla wszystkich platform sprzętowych i programowych, wszystkich maszyn, wszystkich wersji oprogramowania, w tym bez względu na wersję językową oprogramowania – bez względu na to jak duża jest sieć lub jak bardzo jest złożona. 13. Mechanizm określania źródeł ataków prowadzonych przy użyciu zagrożeń hybrydowych.

	14. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji). 15. Obsługa plików skompresowanych obejmująca najpopularniejsze formaty, w tym co najmniej : ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2. 16. Automatyczne usuwanie wirusów oraz oprogramowania typu malware i zgłaszanie alertów w przypadku wykrycia wirusa. 17. Logowanie historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów z poziomu GUI aplikacji. 18. Automatyczne uruchamianie procedur naprawczych. 19. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione. 20. Gwarancja na dostarczenie szczepionki na nowego wirusa w czasie krótszym niż 48 godzin. 21. Średni czas reakcji producenta na nowy wirus poniżej 8 godzin, 24 godziny na dobę przez cały rok (24/7/365). 22. Automatyczne powiadomienie użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem stacja robocza jest odpowiednio zabezpieczona. 23. Skanowanie przez program na komputerze klienckim przychodzącej i wychodzącej poczty elektronicznej bez konieczności instalowania dodatkowych programów/modułów. W programach pocztowych nie modyfikowane są ustawienia konta, tj. serwera POP3, SMTP i IMAP. Obsługuje m.in. MS Outlook Express, MS Outlook, Mozilla, Eudora, Netscape Mail. 24. Skanowanie przez program na komputerze klienckim, danych pobieranych i wysyłanych danych przy pomocy protokołu http. 25. Wsparcie dla technologii Cisco Network Admission Control (NAC). 26. Wsparcie dla technologii Microsoft Network Access Protection (NAP). 27. Ochrona przeglądarki internetowej, w tym: blokowanie wyskakujących okienek, blokowanie ciasteczek (cookies), blokowanie możliwości zmian ustawień w IE, analiza uruchamianych skryptów ActiveX i pobieranych plików. 28. Ochrona podczas przeglądania sieci Internet na podstawie badania reputacji – moduł działający na bazie Network Interceptor Framework (niezależnie od rodzaju i wersji przeglądarki). 29. Możliwość pobierania aktualizacji przez klientów między sobą – tzw. „Neighborcast" pozwalające na odciążenie łącza do sieci WAN. 30. Ochrona rejestrów systemowych, w tym odpowiedzialnych za konfigurację przeglądarki Internet Explorer, listę uruchamianych aplikacji przy starcie, przypisania rozszerzeń plików do zadanych aplikacji. 31. Kontrola oraz możliwość blokowania aplikacji próbujących uzyskać połączenie z Internetem lub siecią lokalną. 32. Osobista zapora ogniowa (tzw. personal firewall) z możliwością definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup roboczych. 33. Moduł kontroli urządzeń zapewniający możliwość zezwolenia lub zabronienia dostępu do komputera urządzeń zewnętrznych (np. napędy usb, urządzenia bluetooth). 34. Moduł kontroli urządzeń zarządzany z poziomu konsoli centralnego zarządzania. 35. Moduł blokowania botnetów. 36. Moduł aktualizacji oprogramowania skanujący stacje robocze pod kontem niezastosowanych łatek systemu Windows i aplikacji firm trzecich oraz ich instalacji z

	poziomu konsoli centralnego zarządzania z możliwością definiowania wykluczeń trybu automatycznego na podstawie nazw programów lub identyfikatorów biuletynów. 37. Moduł kontroli zawartości internetowej umożliwiający ograniczenie dostępu do określonych usług i treści internetowych, a także pozwalający określić treści dostępne dla użytkowników. Wymagania dotyczące systemy zarządzania centralnego: 1. Konsola zarządzania umożliwia eksport pakietu instalacyjnego dla klienta w formacie Microsoft Installer (MSI) i JAR lub też bezpośrednią instalację zdalną nienadzorowaną. 2. Narzędzie instalacyjne musi sprawdzać istnienie poprzednich wersji oprogramowania. W przypadku znalezienia poprzedniej wersji instalator powinien pozostawić ustawienia użytkownika, usunąć starsze oprogramowanie z klienta lub serwera i instalować nowe wersję. 3. Pełna administracja konfiguracją i monitorowanie stacji roboczych i serwerów plików za pomocą konsoli administracyjnej (centralna instalacja, konfiguracja w czasie rzeczywistym, zarządzanie, raportowanie i administrowanie oprogramowaniem). 4. Komunikacja pomiędzy serwerem centralnego zarządzania a stacjami roboczymi musi być zaszyfrowana lub sygnowana stosownymi kluczami prywatnymi i publicznymi. 5. Scentralizowane blokowanie i odblokowywanie dostępu użytkownika do zmian konfiguracyjnych oprogramowania klienckiego, konsola pozwala na zdalne zarządzanie wszystkimi ustawieniami klienta. 6. Administratorzy muszą mieć możliwość tworzenia logicznych grup klientów i serwerów, w celu zarządzania oraz wymuszania określonych dla grupy zasad bezpieczeństwa. 7. Centralna konsola administracyjna musi umożliwiać przenoszenie klientów z jednej grupy do drugiej z możliwością zachowania ustawień lub dziedziczenia ustawień grupy. 8. Możliwość zmiany ustawień dla poszczególnych grup, umożliwienie administratorom zarządzania poszczególnymi klientami i funkcjonalnymi grupami klientów (tworzenie grup klientów). 9. Tworzenie grup, zdalne instalowanie oprogramowania oraz wymuszanie stosowania określonych zasad i ustawień na klientach. 10. Możliwość importu struktury drzewa z Microsoft Active Directory. 11. Możliwość blokowania wszystkich ustawień konfiguracyjnych stacji roboczych w celu uniemożliwienia ich modyfikacji przez użytkowników. 12. Serwer zarządzający związany z konsolą zarządzającą musi mieć funkcję przesyłania aktualizacji do klientów z możliwością ustawienia harmonogramu lub częstotliwości aktualizacji. 13. Możliwość definiowania harmonogramów lub częstotliwości automatycznego pobierania aktualizacji definicji wirusów od producenta oprogramowania przez serwer zarządzający. 14. Możliwość instalacji i konfiguracji wewnętrznego serwera aktualizacji, łączącego się z serwerem aktualizacji producenta i aktualizacja serwerów, serwera zarządzającego oraz stacji roboczych z wewnętrznego serwera aktualizacji. 15. Możliwość ustalenia dodatkowego harmonogramu pobierania przez serwery plików i stacje robocze aktualizacji z serwera producenta. 16. Funkcja przechowywania i przekazywania danych umożliwiająca przechowywanie przez klientów danych dotyczących zdarzeń, w sytuacji, jeśli nie mogą oni uzyskać połączenia z serwerem zarządzania. 17. Dane powinny być przesyłane do serwera zarządzania podczas kolejnego połączenia. 18. Możliwość włączania/wyłączania wyświetlania komunikatów o znalezionych wirusach na wybranych stacjach klienckich.

	19. Program musi pozwalać administratorowi zdefiniować treść komunikatu wyświetlanego w przypadku wykrycia wirusa. 20. Umożliwienie administratorom na audyt sieci, polegający na wykryciu niechronionych węzłów narażonych na ataki wirusowe. 21. Automatyczne wykrywanie i usuwanie oprogramowanie innych wiodących producentów systemów antywirusowych (min. 3 inne) podczas instalacji. 22. Automatyczne uaktualnianie bazy definicji wirusów oraz mechanizmów skanujących nie rzadziej niż co 7 dni (zalecane codzienne aktualizacje). 23. Automatyczne pobieranie przez program antywirusowy klienta zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe. 24. Możliwość eksportu raportów z pracy systemu do pliku csv i html. 25. Możliwość natychmiastowej aktualizacji przez serwer definicji wirusów na stacjach klienckich. 26. Możliwość uruchomienia aktualizacji stacji roboczych i serwerów przez użytkowników „na żądanie”. 27. Program musi pozwalać administratorowi na określenie reakcji w przypadku wykrycia wirusa. 28. Program musi pozwalać na określenie obszarów skanowania, tj.: pliki, katalogi, napędy lokalne i sieciowe. 29. Program musi pozwalać na skanowanie pojedynczych plików przez dodanie odpowiedniej opcji do menu kontekstowego (po kliknięciu prawym przyciskiem myszy). 30. Program musi pozwalać na określenie typów skanowanych plików, momentu ich skanowania (otwarcie, modyfikacja) oraz na wykluczenie ze skanowania określonych folderów. 31. Zarządzanie zdarzeniami i raportowanie – natychmiastowe alarmowanie o aktywności wirusów w administrowanej sieci na kilka sposobów: poczta elektroniczna, powiadomienia przez SNMP, raportowanie do dziennika systemowego, raportowanie do systemu centralnego zarządzania. 32. Możliwość tworzenia wielu kont dostępu do systemu centralnego zarządzania dla różnych użytkowników (w tym możliwość nadaniu danemu użytkownikowi ograniczonych praw).
Pakiet Biurowy	Pakiet biurowy dostarczony wraz z licencją i nośnikiem. • Wymagania odnośnie interfejsu użytkownika: o Pełna polska wersja językowa interfejsu użytkownika. o Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się. • Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: o posiada kompletny i publicznie dostępny opis formatu, o ma zdefiniowany układ informacji w postaci XML zgodnie z Tabelą B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2005.212.1766), o umożliwia wykorzystanie schematów XML, wspiera w swojej specyfikacji podpis elektroniczny zgodnie z Tabelą A.1.1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2005.212.1766)

	• Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców. • W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy), • Do aplikacji musi być dostępna pełna dokumentacja w języku polskim. • Pakiet zintegrowanych aplikacji biurowych musi zawierać: o Edytor tekstów o Arkusz kalkulacyjny o Narzędzie do przygotowywania i prowadzenia prezentacji o Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) • Edytor tekstów musi umożliwiać: o Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty. o Wstawianie oraz formatowanie tabel i obiektów graficznych. o Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne). o Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel, rysunków oraz tworzenie spisów treści. o Formatowanie nagłówków i stopek stron. o Sprawdzanie pisowni w języku polskim. o Śledzenie zmian wprowadzonych przez użytkowników. o Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. o Określenie układu strony (pionowa/pozioma). o Wydruk dokumentów. o Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną. o Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003, 2007, 2010 i 2013 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów Dokumentu. o Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. o Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem. o Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa. o Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze pozwalające zapisać plik wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i Prawnych. • Arkusz kalkulacyjny musi umożliwiać:

	o Tworzenie raportów tabelarycznych i wykresów liniowych (wraz linią trendu), słupkowych, kołowych. o Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu. o Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice). o Obsługę „kostek OLAP" oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych. o Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych. o Wyszukiwanie i zamianę danych. o Wykonywanie analiz danych przy użyciu formatowania warunkowego. o Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie. o Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. o Formatowanie czasu, daty i wartości finansowych z polskim formatem. o Zapis wielu arkuszy kalkulacyjnych w jednym pliku. o Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003, 2007, 2010 i 2013 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń. o Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. • Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: o Przygotowywanie prezentacji multimedialnych, które będą: – Prezentowane przy użyciu projektora multimedialnego. – Drukowane w formacie umożliwiającym robienie notatek. – Zapisane jako prezentacja tylko do odczytu. o Nagrywanie narracji i dołączanie jej do prezentacji. o Opatrywanie slajdów notatkami dla prezentera. o Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo. o Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego. o Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym. o Możliwość tworzenia animacji obiektów i całych slajdów. o Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera. o Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, 2007 2010 i 2013. • Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: o Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego. o Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców. o Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną. o Automatyczne grupowanie poczty o tym samym tytule.

	o Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy. o Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia. o Zarządzanie kalendarzem. o Udostępnianie kalendarza innym użytkownikom. o Przeglądanie kalendarza innych użytkowników. o Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach. o Zarządzanie listą zadań. o Zlecanie zadań innym użytkownikom. o Zarządzanie listą kontaktów. o Udostępnianie listy kontaktów innym użytkownikom. o Przeglądanie listy kontaktów innych użytkowników. o Możliwość przesyłania kontaktów innym użytkowników.

Monitor – 15 szt.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne monitora
1.	Typ ekranu	Ekran ciekłokrystaliczny z aktywną matrycą WLED/VA lub IPS 21,5”
2.	Rozmiar plamki	0,248 mm
3.	Jasność	250 cd/m2
4.	Kąty widzenia (pion/poziom)	178(H)/178(V) stopni
5.	Czas reakcji matrycy	max 5 ms
6.	Rozdzielczość maksymalna	1920 x 1080 przy 60Hz
7.	Wyświetlane kolory	16.7 milionów
8.	Częstotliwość odświeżania poziomego	24 – 80 kHz
9.	Pochylenie monitora	W zakresie 25 stopni
10.	Powłoka powierzchni ekranu	Antyodblaskowa
11.	Podświetlenie	System podświetlenia LED
12.	Zużycie energii	Typowo max 23W, czuwanie mniej niż 0,5W
13.	Bezpieczeństwo	Monitor musi być wyposażony w złącze (gniazdo) pozwalające zabezpieczyć go przed kradzieżą.
14.	Złącze	1x 15-stykowe złącze D-Sub, 1x złącze HDMI, Audio : Mini-jack 3,5mm
15.	Gwarancja	Min. 3-letnia gwarancja (trzy letnia lub dłużej zgodnie ze złożoną ofertą), świadczona na miejscu u klienta, czas reakcji serwisu - do końca następnego dnia roboczego.
16.	Certyfikaty	TCO 6.0, Energy Star 6.0, lub równoważne.
17.	Inne	Odłączana stopa; Dwa wbudowane w obudowę monitora dedykowane głośniki o mocy min. 2W stereo RMS. Kabel HDMI do połączenia monitora z komputerem o długości 2m.

1.3.3 KOMPUTERY PRZENOŚNE DLA RADNYCH

Laptop – 15 szt.

Nazwa	Wymagane minimalne parametry techniczne
Konstrukcja/obudowa	Komputer przenośny typu Ultrabook będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej.
Przekątna Ekranu	Ekran o przekątnej minimum 13,3" o rozdzielczości FHD (1920x1080 pikseli) Matryca antyodblaskowa z podświetlaniem LED, IPS o jasności minimum 300 nitów.
Wydajność	Oferowany procesor powinien osiągać w teście wydajności Passmark CPU Mark wynik co najmniej 3490 punktów. Dokumentem potwierdzającym spełnianie ww. wymagań będzie wydruk ze strony https://www.cpubenchmark.net/cpu_list.php Dokumenty potwierdzające spełnienie powyższych wymagań załączyć na wezwanie Zamawiającego zgodnie z art. 26 ust. 2 ustawy prawo zamówień publicznych.
Pamięć RAM	4GB z możliwością rozbudowy do 16GB RAM; min. jeden slot wolny;
Pamięć masowa	1szt. 128GB SSD lub równoważny oraz 1szt. 500GB HDD
Karta graficzna	Zintegrowana w procesorze z możliwością dynamicznego przydzielenia pamięci systemowej, ze sprzętowym wsparciem dla DirectX 12, Shader 5.0 posiadająca minimum 2.0EU (Graphics ExecutionUnits).
Klawiatura	Klawiatura podświetlana wyspowa odporna na zalanie cieczą(materiał pod klawiaturą wchłaniający wilgoć i ciecz), Powłoka antybakteryjna. Touchpad wyposażony w 2 niezależne klawisze funkcyjne ze wsparciem dla technologii multitouch. Musi posiadać wsparcie dla gestów dla minimum 3 niezależnych punktów dotyku.
Multimedia	czterokanałowa (24-bitowa) karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowany głośniki o średniej mocy min. 2W, Dwa kierunkowe, cyfrowe mikrofony z funkcja redukcji szumów i poprawy mowy wbudowane w obudowę matrycy. Kamera internetowa trwale zainstalowana w obudowie matrycy oraz dioda LED.
Bateria i zasilanie	Min. 3-cell 48 Whr Litowo-polimerowa. Umożliwiająca jej szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin. Zasilacz o mocy maks. 45W
Waga i wymiary	Waga max 2 kg z baterią Ultrabook posiadający po złożeniu wysokość maksymalnie 35 mm
Obudowa	Obudowa notebooka wzmocniona z zewnątrz aluminium. Szkielet i zawiasy notebooka wykonany z wzmacnianego metalu.
BIOS	Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o: Wersji BIOS. Numerze seryjnym komputera. Ilości pamięci RAM. Modelu procesora oraz częstotliwości jego taktowania. Modelu dysku twardego Modelu napędu optycznego Możliwość wyłączenia zintegrowanego touchpada. Możliwość wyłączenia karty LAN. Możliwość wyłączenia karty WLAN.

	Możliwość wyłączenia napędu optycznego. Możliwość wyłączenia czytnika kart. Możliwość wyłączenia portów USB. Możliwość wyłączenia zintegrowanej kamery. • Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń. • Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z USB • 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 systemowym 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.
Certyfikaty	• Certyfikat ISO9001 dla producenta sprzętu lub równoważne • Deklaracja zgodności CE lub równoważne • Potwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym • Certyfikat EnergyStar 6.0 Dokumenty potwierdzające spełnienie powyższych wymagań załączyć na wezwanie Zamawiającego zgodnie z art. 26 ust. 2 ustawy prawo zamówień publicznych.
Bezpieczeństwo	Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej. Czujnik spadania zwiększający ochronę dysków twardych działający nawet przy wyłączonym notebooku oraz konstrukcja absorbująca wstrząsy.
System operacyjny	Zainstalowany system musi spełniać następujące wymagania, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: • 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) – wymagane podanie nazwy strony serwera WWW; • Internetowa aktualizacja zapewniona w języku polskim; • Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; • Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, 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 służącą 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. • Funkcjonalność rozpoznawania mowy, pozwalającą 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 (np. słabo widzących); • 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; • 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 i 2.0 i 3.0 – 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 za logowanego 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 ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację; • Graficzne środowisko instalacji i konfiguracji; • Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) 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. • 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 (np. przy użyciu numerów identyfikacyjnych sprzętu).
Dodatkowe oprogramowa-nie	Oprogramowanie producenta umożliwiające zrobienie kopii zapasowej instalatora systemu operacyjnego na pamięci zewnętrznej. Oprogramowanie producenta do automatycznej aktualizacji preinstalowanego oprogramowania producenta jak i sterowników dziejąca w tle. Oprogramowanie producenta komputera służące do rozpoznawania niezależnych gestów wykonywanych jednym, dwoma i trzema palcami na zintegrowanym Touchpadzie. Pozwalające na automatyczne wyłączenie zintegrowanego Touch pada w momencie podpięcie zewnętrznej myszki do portu USB. Oprogramowanie producenta komputera informujące użytkownika o problemach ze złączem zasilania zabezpieczające przed zwarciem w wtyku zasilającym. Oprogramowanie producenta komputera umożliwiające zablokowanie uruchomienia danego typu urządzeń zewnętrznych (podział Audio/Video, zewnętrzne nośniki danych, urządzenia biurowe – skanery, drukarki itd., inne urządzenia), umożliwiające analizę systemu w celu zdiagnozowania potencjalnych usterek (CPU,GPU, HDD, RAM) Oprogramowanie producenta komputera umożliwiające ładowanie urządzeń zewnętrznych poprzez dedykowany port USB nawet w przypadku gdy notebook jest wyłączony i w trybie hibernacji.
Porty i złącza	Wbudowane porty i złącza : - 1x HDMI - 2x USB 2.0 - 1x USB 3.0 - 1x RJ-45 (10/100/1000) - czytnik kart multimedialny wspierający karty SD 4.0 - współdzielone złącze słuchawkowe stereo i złącze mikrofonowe tzw. combo - port zasilania
Warunki gwarancji	Min. 3-letnia gwarancja (trzy letnia lub dłużej zgodnie ze złożoną ofertą), świadczona na miejscu u klienta, czas reakcji serwisu - do końca następnego dnia roboczego.
Antywirus	Istotne cechy oprogramowania: 1. Ochrona antywirusowa stacji roboczych pracujących pod kontrolą systemów operacyjnych Windows 7, 8, 8.1, 10 w wersjach 32-bit oraz 64-bit oraz dostarczonym z zaoferowanym w ramach niniejszego postępowania. 2. Ochrona antywirusowa wyżej wymienionych systemów zarządzana i monitorowana z pojedynczej, centralnej konsoli. 3. Serwer konsoli zarządzania pracujący pod kontrolą wymienionych niżej systemów: - Windows Server 2008 SP1 (32-bit) edycji Standard, Enterprise oraz Web Server - Windows Server 2008 SP1 (64-bit) edycji Standard, Enterprise, Web Server, Small Bussines Server oraz Essential Bussines Server - Windows Server 2008 R2 oraz Windows Server 2008 R2 SP1 edycji Standard, Enterprise oraz Web Server - Windows Server 2012 edycji Essentials, Standard oraz Datacenter - Windows Server 2012 R2 edycji Essentials, Standard oraz Datacenter

	- Windows Server 2016 edycji Essentials, Standard oraz Datacenter - Red Hat Enterprise Linux 5, 6 and 7 (32-bit oraz b4-bit) - CentOS 6, 7(32-bit oraz b4-bit) - openSUSE 13.2 (32-bit oraz b4-bit) - SUSELinuxEnterpriseServer10 and 11 (32-bit oraz b4-bit) - SUSE Linux Enterprise Desktop 11 (32-bit oraz b4-bit) - Debian GNU Linux 7 and 8 (32-bit oraz b4-bit) - Ubuntu 12.04, 14.04, 16.04 (32-bit oraz b4-bit) 4. Konsola zarządzania pracująca pod kontrolą wymienionych niżej systemów: - Windows 7 i Windows 7 SP1 (32-bit oraz 64-bit) edycji Professional, Enterprise oraz Ultimate - Windows 8 (32-bit oraz 64-bit) wszystkie edycje - Windows 8.1 (32-bit oraz 64-bit) wszystkie edycje - Windows 10 (32-bit oraz 64-bit) - Windows Server 2008 SP1 (32-bit) edycji Standard, Enterprise oraz Web Server - Windows Server 2008 SP1 (64-bit) edycji Standard, Enterprise, Web Server, Small Bussines Server oraz Essential Bussines Server - Windows Server 2008 R2 oraz Windows Server 2008 R2 SP1 edycji Standard, Enterprise oraz Web Server - Windows Server 2012 edycji Essentials, Standard oraz Datacenter - Windows Server 2012 R2 edycji Essentials, Standard oraz Datacenter - Windows Server 2016 edycji Essentials, Standard oraz Datacenter - Red Hat Enterprise Linux 5, 6 and 7 (32-bit oraz 64-bit) - CentOS 6, 7 (32-bit oraz b4-bit) - openSUSE 13.2 (32-bit oraz b4-bit) - SUSE Linux Enterprise Server 10 and 11 (32-bit oraz b4-bit) - SUSE Linux Enterprise Desktop 11 (32-bit oraz b4-bit) - Debian GNU Linux 7 and 8 (32-bit oraz b4-bit) - Ubuntu 12.04, 14.04, 16.04 (32-bit oraz b4-bit) 5. Możliwość instalacji konsoli zarządzania niezależnie na kilku wybranych stacjach. 6. Polski interfejs użytkownika i dokumentacja do oprogramowania na stację roboczą. Wymagania dotyczące technologii: 1. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanującego nośniki i monitora poczty elektronicznej, monitora ruchu http oraz moduł antyrootkitowy. 2. Co najmniej trzy różne silniki antywirusowe, funkcjonujące jednocześnie i skanujące wszystkie dane. 3. Oddzielny silnik skanujący do wykrywania niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan". 4. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie. 5. Możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta. 6. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie. 7. Brak konieczności restartu komputerów po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów. 8. Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.

	9. Wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan", „rootkit". 10. Możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger", „dialer", „trojan" w kwarantannie. 11. Mechanizm centralnego zarządzania folderami kwarantanny znajdującymi się na stacjach klienckich. 12. Mechanizm skanujący wspólny dla wszystkich platform sprzętowych i programowych, wszystkich maszyn, wszystkich wersji oprogramowania, w tym bez względu na wersję językową oprogramowania – bez względu na to jak duża jest sieć lub jak bardzo jest złożona. 13. Mechanizm określania źródeł ataków prowadzonych przy użyciu zagrożeń hybrydowych. 14. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji). 15. Obsługa plików skompresowanych obejmująca najpopularniejsze formaty, w tym co najmniej : ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2. 16. Automatyczne usuwanie wirusów oraz oprogramowania typu malware i zgłaszanie alertów w przypadku wykrycia wirusa. 17. Logowanie historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów z poziomu GUI aplikacji. 18. Automatyczne uruchamianie procedur naprawczych. 19. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione. 20. Gwarancja na dostarczenie szczepionki na nowego wirusa w czasie krótszym niż 48 godzin. 21. Średni czas reakcji producenta na nowy wirus poniżej 8 godzin, 24 godziny na dobę przez cały rok (24/7/365). 22. Automatyczne powiadomienie użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem stacja robocza jest odpowiednio zabezpieczona. 23. Skanowanie przez program na komputerze klienckim przychodzącej i wychodzącej poczty elektronicznej bez konieczności instalowania dodatkowych programów/modułów. W programach pocztowych nie modyfikowane są ustawienia konta, tj. serwera POP3, SMTP i IMAP. Obsługuje m.in. MS Outlook Express, MS Outlook, Mozilla, Eudora, Netscape Mail. 24. Skanowanie przez program na komputerze klienckim, danych pobieranych i wysyłanych danych przy pomocy protokołu http. 25. Wsparcie dla technologii Cisco Network Admission Control (NAC). 26. Wsparcie dla technologii Microsoft Network Access Protection (NAP). 27. Ochrona przeglądarki internetowej, w tym: blokowanie wyskakujących okienek, blokowanie ciasteczek (cookies), blokowanie możliwości zmian ustawień w IE, analiza uruchamianych skryptów ActiveX i pobieranych plików. 28. Ochrona podczas przeglądania sieci Internet na podstawie badania reputacji – moduł działający na bazie Network Interceptor Framework (niezależnie od rodzaju i wersji przeglądarki). 29. Możliwość pobierania aktualizacji przez klientów między sobą – tzw. „Neighborcast" pozwalające na odciążenie łącza do sieci WAN.

	30. Ochrona rejestrów systemowych, w tym odpowiedzialnych za konfigurację przeglądarki Internet Explorer, listę uruchamianych aplikacji przy starcie, przypisania rozszerzeń plików do zadanych aplikacji. 31. Kontrola oraz możliwość blokowania aplikacji próbujących uzyskać połączenie z Internetem lub siecią lokalną. 32. Osobista zapora ogniowa (tzw. personal firewall) z możliwością definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup roboczych. 33. Moduł kontroli urządzeń zapewniający możliwość zezwolenia lub zabronienia dostępu do komputera urządzeń zewnętrznych (np. napędy usb, urządzenia bluetooth). 34. Moduł kontroli urządzeń zarządzany z poziomu konsoli centralnego zarządzania. 35. Moduł blokowania botnetów. 36. Moduł aktualizacji oprogramowania skanujący stacje robocze pod kontem niezastosowanych łatek systemu Windows i aplikacji firm trzecich oraz ich instalacji z poziomu konsoli centralnego zarządzania z możliwością definiowania wykluczeń trybu automatycznego na podstawie nazw programów lub identyfikatorów biuletynów. 37. Moduł kontroli zawartości internetowej umożliwiający ograniczenie dostępu do określonych usług i treści internetowych, a także pozwalający określić treści dostępne dla użytkowników. Wymagania dotyczące systemy zarządzania centralnego: 1. Konsola zarządzania umożliwia eksport pakietu instalacyjnego dla klienta w formacie Microsoft Installer (MSI) i JAR lub też bezpośrednią instalację zdalną nienadzorowaną. 2. Narzędzie instalacyjne musi sprawdzać istnienie poprzednich wersji oprogramowania. W przypadku znalezienia poprzedniej wersji instalator powinien pozostawić ustawienia użytkownika, usunąć starsze oprogramowanie z klienta lub serwera i instalować nowe wersję. 3. Pełna administracja konfiguracją i monitorowanie stacji roboczych i serwerów plików za pomocą konsoli administracyjnej (centralna instalacja, konfiguracja w czasie rzeczywistym, zarządzanie, raportowanie i administrowanie oprogramowaniem). 4. Komunikacja pomiędzy serwerem centralnego zarządzania a stacjami roboczymi musi być zaszyfrowana lub sygnowana stosownymi kluczami prywatnymi i publicznymi. 5. Scentralizowane blokowanie i odblokowywanie dostępu użytkownika do zmian konfiguracyjnych oprogramowania klienckiego, konsola pozwala na zdalne zarządzanie wszystkimi ustawieniami klienta. 6. Administratorzy muszą mieć możliwość tworzenia logicznych grup klientów i serwerów, w celu zarządzania oraz wymuszania określonych dla grupy zasad bezpieczeństwa. 7. Centralna konsola administracyjna musi umożliwiać przenoszenie klientów z jednej grupy do drugiej z możliwością zachowania ustawień lub dziedziczenia ustawień grupy. 8. Możliwość zmiany ustawień dla poszczególnych grup, umożliwienie administratorom zarządzania poszczególnymi klientami i funkcjonalnymi grupami klientów (tworzenie grup klientów). 9. Tworzenie grup, zdalne instalowanie oprogramowania oraz wymuszanie stosowania określonych zasad i ustawień na klientach. 10. Możliwość importu struktury drzewa z Microsoft Active Directory. 11. Możliwość blokowania wszystkich ustawień konfiguracyjnych stacji roboczych w celu uniemożliwienia ich modyfikacji przez użytkowników. 12. Serwer zarządzający związany z konsolą zarządzającą musi mieć funkcję przesyłania aktualizacji do klientów z możliwością ustawienia harmonogramu lub częstotliwości aktualizacji.

	13. Możliwość definiowania harmonogramów lub częstotliwości automatycznego pobierania aktualizacji definicji wirusów od producenta oprogramowania przez serwer zarządzający. 14. Możliwość instalacji i konfiguracji wewnętrznego serwera aktualizacji, łączącego się z serwerem aktualizacji producenta i aktualizacja serwerów, serwera zarządzającego oraz stacji roboczych z wewnętrznego serwera aktualizacji. 15. Możliwość ustalenia dodatkowego harmonogramu pobierania przez serwery plików i stacje robocze aktualizacji z serwera producenta. 16. Funkcja przechowywania i przekazywania danych umożliwiająca przechowywanie przez klientów danych dotyczących zdarzeń, w sytuacji, jeśli nie mogą oni uzyskać połączenia z serwerem zarządzania. 17. Dane powinny być przesyłane do serwera zarządzania podczas kolejnego połączenia. 18. Możliwość włączania/wyłączania wyświetlania komunikatów o znalezionych wirusach na wybranych stacjach klienckich. 19. Program musi pozwalać administratorowi zdefiniować treść komunikatu wyświetlanego w przypadku wykrycia wirusa. 20. Umożliwienie administratorom na audyt sieci, polegający na wykryciu niechronionych węzłów narażonych na ataki wirusowe. 21. Automatyczne wykrywanie i usuwanie oprogramowanie innych wiodących producentów systemów antywirusowych (min. 3 inne) podczas instalacji. 22. Automatyczne uaktualnianie bazy definicji wirusów oraz mechanizmów skanujących nie rzadziej niż co 7 dni (zalecane codzienne aktualizacje). 23. Automatyczne pobieranie przez program antywirusowy klienta zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe. 24. Możliwość eksportu raportów z pracy systemu do plikucsv i html. 25. Możliwość natychmiastowej aktualizacji przez serwer definicji wirusów na stacjach klienckich. 26. Możliwość uruchomienia aktualizacji stacji roboczych i serwerów przez użytkowników „na żądanie”. 27. Program musi pozwalać administratorowi na określenie reakcji w przypadku wykrycia wirusa. 28. Program musi pozwalać na określenie obszarów skanowania, tj.: pliki, katalogi, napędy lokalne i sieciowe. 29. Program musi pozwalać na skanowanie pojedynczych plików przez dodanie odpowiedniej opcji do menu kontekstowego (po kliknięciu prawym przyciskiem myszy). 30. Program musi pozwalać na określenie typów skanowanych plików, momentu ich skanowania (otwarcie, modyfikacja) oraz na wykluczenie ze skanowania określonych folderów. 31. Zarządzanie zdarzeniami i raportowanie – natychmiastowe alarmowanie o aktywności wirusów w administrowanej sieci na kilka sposobów: poczta elektroniczna, powiadomienia przez SNMP, raportowanie do dziennika systemowego, raportowanie do systemu centralnego zarządzania. 32. Możliwość tworzenia wielu kont dostępu do systemu centralnego zarządzania dla różnych użytkowników (w tym możliwość nadaniu danemu użytkownikowi ograniczonych praw).
Pakiet biurowy	Pakiet biurowy dostarczony wraz z licencją i nośnikiem. • Wymagania odnośnie interfejsu użytkownika: o Pełna polska wersja językowa interfejsu użytkownika.

	o Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych. o Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się. • Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: o posiada kompletny i publicznie dostępny opis formatu, o ma zdefiniowany układ informacji w postaci XML zgodnie z Tabelą B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2005.212.1766), o umożliwia wykorzystanie schematów XML, wspiera w swojej specyfikacji podpis elektroniczny zgodnie z Tabelą A.1.1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2005.212.1766) • Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców. • W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy), • Do aplikacji musi być dostępna pełna dokumentacja w języku polskim. • Pakiet zintegrowanych aplikacji biurowych musi zawierać: o Edytor tekstów o Arkusz kalkulacyjny o Narzędzie do przygotowywania i prowadzenia prezentacji o Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) • Edytor tekstów musi umożliwiać: o Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty. o Wstawianie oraz formatowanie tabel i obiektów graficznych. o Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne). o Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel, rysunków oraz tworzenie spisów treści. o Formatowanie nagłówków i stopek stron. o Sprawdzanie pisowni w języku polskim. o Śledzenie zmian wprowadzonych przez użytkowników. o Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. o Określenie układu strony (pionowa/pozioma). o Wydruk dokumentów. o Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.

	o Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003, 2007, 2010 i 2013 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów Dokumentu. o Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. o Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem. o Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa. o Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze pozwalające zapisać plik wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i Prawnych. • Arkusz kalkulacyjny musi umożliwiać: o Tworzenie raportów tabelarycznych i wykresów liniowych (wraz linią trendu), słupkowych, kołowych. o Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu. o Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice). o Obsługę „kostek OLAP” oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych. o Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych. o Wyszukiwanie i zamianę danych. o Wykonywanie analiz danych przy użyciu formatowania warunkowego. o Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie. o Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. o Formatowanie czasu, daty i wartości finansowych z polskim formatem. o Zapis wielu arkuszy kalkulacyjnych w jednym pliku. o Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003, 2007, 2010 i 2013 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń. o Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. • Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: o Przygotowywanie prezentacji multimedialnych, które będą: – Prezentowane przy użyciu projektora multimedialnego. – Drukowane w formacie umożliwiającym robienie notatek. – Zapisane jako prezentacja tylko do odczytu.

	o Nagrywanie narracji i dołączanie jej do prezentacji. o Opatrywanie slajdów notatkami dla prezentera. o Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo. o Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego. o Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym. o Możliwość tworzenia animacji obiektów i całych slajdów. o Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera. o Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, 2007 2010 i 2013. • Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: o Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego. o Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców. o Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną. o Automatyczne grupowanie poczty o tym samym tytule. o Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy. o Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia. o Zarządzanie kalendarzem. o Udostępnianie kalendarza innym użytkownikom. o Przeglądanie kalendarza innych użytkowników. o Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach. o Zarządzanie listą zadań. o Zlecanie zadań innym użytkownikom. o Zarządzanie listą kontaktów. o Udostępnianie listy kontaktów innym użytkownikom. o Przeglądanie listy kontaktów innych użytkowników. Możliwość przesyłania kontaktów innym użytkowników.

1.3.4 KOMPUTERY PRZENOŚNE DLA KADRY ZARZĄDZAJĄCEJ I PRACOWNIKÓW OBSŁUGI RADY GMINY

Laptop – 5 szt. (dla kadry zarządzającej i pracowników administracyjnych)

Nazwa	Wymagane minimalne parametry techniczne
Zastosowanie	Komputer przenośny będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna
Ekran	Ekran o przekątnej minimum 17" o rozdzielczości FHD (1920×1080 pikseli.) Matryca matowa antyodblaskowa z podświetlaniem LED o jasności minimum 250 nitów. Kontrast minimum 400:1.
Procesor	Oferowany procesor powinien osiągać w teście wydajności Passmark CPU Mark, wynik co najmniej 8400 punktów.

	Dokumentem potwierdzającym spełnianie ww. wymagań będzie wydruk ze strony https://www.cpubenchmark.net/cpu_list.php; Dokumenty potwierdzające spełnienie powyższych wymagań załączyć na wezwanie Zamawiającego zgodnie z art. 26 ust. 2 ustawy prawo zamówień publicznych.
Pamięć RAM	8GB z możliwością rozbudowy do min. 16GB.
Pamięć masowa	1szt. 128GB SSD lub równoważny oraz 1szt. 500GB.
Karta graficzna	Zintegrowana w procesorze z możliwością dynamicznego przydzielenia pamięci systemowej, ze sprzętowym wsparciem dla DirectX 12, Shader 5.0 posiadająca minimum 20EU (Graphics ExecutionUnits).
Napęd optyczny	Wbudowany w obudowę DVD+/-RW
Klawiatura i touchpad	Klawiatura z wydzieloną sekcją numeryczną po prawej stronie, powłoka antybakteryjna, odporna na zalanie cieczą (materiał pod klawiaturą wchłaniający wilgoć i ciecz). Klawiatura w układzie US-QWERTY), musi posiadać minimum 102 klawisze. Touchpad wyposażony w 2 niezależne klawisze funkcyjne ze wsparciem dla technologii multitouch. Musi posiadać wsparcie dla gestów dla minimum 3 niezależnych punktów dotyku.
Multimedia	Czterokanałowa (24-bitowa) karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane głośniki stereo o mocy min. 3W Mikrofon z funkcja redukcji szumów i poprawy mowy wbudowane w obudowę matrycy. Kamera internetowa trwale zainstalowana w obudowie matrycy wraz diodą LED.
Bateria i zasilanie	Litowo-polimerowa min. 2-cell 38 Whrs. Osiągająca w teście MobileMark 2014 Office Productivity Battery Life: min. 300 minutes Umożliwiająca jej szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin. Zasilacz o mocy min. 65W 2 lata gwarancji na baterię.
Obudowa	Szkielet i zawiasy notebooka wykonany z wzmacnianego metalu. Obudowa wyposażona w diody informujące użytkownika o: - włączonym lub wyłączonym module Wi-fi. - aktywności dysku twardego - ładowaniu oraz naładowaniu baterii (2 niezależne kolory) - włączonym urządzeniu - aktywności włączonej kamery
BIOS	Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o: - Wersji BIOS. - Numerze seryjnym komputera. - Ilości pamięci RAM. - Możliwość wyłączenia zintegrowanego touchpada. - Możliwość wyłączenia karty LAN. - Możliwość wyłączenia karty WLAN. - Możliwość wyłączenia napędu optycznego. - Możliwość wyłączenia czytnika kart. - Możliwość wyłączenia portów USB. - Możliwość wyłączenia zintegrowanej kamery. - Możliwość wyłączenia czytnika linii papilarnych • Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń.

	• Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z USB • 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 systemowym 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.
Certyfikaty	• Certyfikat ISO9001 dla producenta sprzętu lub równoważne • Deklaracja zgodności CE lub równoważne • Potwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym • Certyfikat EnergyStar 6.0 Dokumenty potwierdzające spełnienie powyższych wymagań załączyć na wezwanie Zamawiającego zgodnie z art. 26 ust. 2 ustawy prawo zamówień publicznych.
Bezpieczeństwo	Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej. Czujnik spadania zwiększający ochronę dysków twardych działający nawet przy wyłączonym notebooku oraz konstrukcja absorbująca wstrząsy.
System operacyjny	Zainstalowany system musi spełniać następujące wymagania, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: • 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) – wymagane podanie nazwy strony serwera WWW; • Internetowa aktualizacja zapewniona w języku polskim; • Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; • Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, 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 służącą 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. • Funkcjonalność rozpoznawania mowy, pozwalającą 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 (np. słabo widzących); • 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; • 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 i 2.0 i 3.0 – 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 za logowanego 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 ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację; • Graficzne środowisko instalacji i konfiguracji; • Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) 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. • 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 (np. przy użyciu numerów identyfikacyjnych sprzętu).

Dodatkowe oprogramowanie	Oprogramowanie producenta umożliwiające zrobienie kopii zapasowej instalatora systemu operacyjnego na pamięci zewnętrznej Oprogramowanie producenta do automatycznej aktualizacji preinstalowanego oprogramowania producenta jak i sterowników dziejąca w tle. Oprogramowanie producenta komputera służące do rozpoznawania niezależnych gestów wykonywanych jednym, dwoma i trzema palcami na zintegrowanym Touchpadzie. Pozwalające na automatyczne wyłączenie zintegrowanego Touch pada w momencie podpięcie zewnętrznej myszki do portu USB. Oprogramowanie producenta komputera informujące użytkownika o problemach ze złączem zasilania zabezpieczające przed zwarciem w wtyku zasilającym. Oprogramowanie producenta komputera umożliwiające zablokowanie uruchomienia danego typu urządzeń zewnętrznych (podział Audio/Video, zewnętrzne nośniki danych, urządzenia biurowe – skanery, drukarki itd, inne urządzenia) Oprogramowanie producenta komputera zwiększające ochronę dysku w 3 niezależnych poziomach czułości z graficznym interfejsem użytkownika. Oprogramowanie producenta komputera umożliwiające ładowanie urządzeń zewnętrznych poprzez dedykowany port USB nawet w przypadku gdy notebook jest wyłączony i w trybie hibernacji.
Porty i złącza	Wbudowane porty i złącza : - 1x 15-pin VGA - 1x HDMI ver. 1.4 - 1x RJ-45 (10/100/1000) z funkcją Wake-on-LAN (WOL) umożliwia włączenie komputera za pomocą prostego komunikatu sieciowego - 3 USB w tym: 1x USB 3.0, 2x USB 2.0 (możliwość ładowania urządzeń zewnętrznych poprzez port USB, nawet gdy notebook jest wyłączony i jest w trybie hibernacji/uśpienia) - czytnik kart multimedialny 4in1 wspierający karty SD 4.0 - współdzielone złącze słuchawkowe stereo i złącze mikrofonowe tzw. combo - moduł bluetooth 4.0 - Zintegrowana w postaci wewnętrznego modułu mini-PCI Express karta sieci WLAN obsługująca łącznie standardy IEEE 802.11 a/b/g/n.
Warunki gwarancji	Min. 3-letnia gwarancja (trzy letnia lub dłużej zgodnie ze złożoną ofertą), świadczona na miejscu u klienta, czas reakcji serwisu - do końca następnego dnia roboczego.
Antywirus	Istotne cechy oprogramowania: 1. Ochrona antywirusowa stacji roboczych pracujących pod kontrolą systemów operacyjnych Windows 7, 8, 8.1, 10 w wersjach 32-bit oraz 64-bit oraz dostarczonym z zaoferowanym w ramach niniejszego postępowania. 2. Ochrona antywirusowa wyżej wymienionych systemów zarządzana i monitorowana z pojedynczej, centralnej konsoli. 3. Serwer konsoli zarządzania pracujący pod kontrolą wymienionych niżej systemów: - Windows Server 2008 SP1 (32-bit) edycji Standard, Enterprise oraz Web Server - Windows Server 2008 SP1 (64-bit) edycji Standard, Enterprise, Web Server, Small Bussines Server oraz Essential Bussines Server - Windows Server 2008 R2 oraz Windows Server 2008 R2 SP1 edycji Standard, Enterprise oraz Web Server - Windows Server 2012 edycji Essentials, Standard oraz Datacenter - Windows Server 2012 R2 edycji Essentials, Standard oraz Datacenter - Windows Server 2016 edycji Essentials, Standard oraz Datacenter

	- Red Hat Enterprise Linux 5, 6 and 7 (32-bit oraz b4-bit) - CentOS 6, 7(32-bit oraz b4-bit) - openSUSE 13.2 (32-bit oraz b4-bit) - SUSELinuxEnterpriseServer10 and 11 (32-bit oraz b4-bit) - SUSE Linux Enterprise Desktop 11 (32-bit oraz b4-bit) - Debian GNU Linux 7 and 8 (32-bit oraz b4-bit) - Ubuntu 12.04, 14.04, 16.04 (32-bit oraz b4-bit) 4. Konsola zarządzania pracująca pod kontrolą wymienionych niżej systemów: - Windows 7 i Windows 7 SP1 (32-bit oraz 64-bit) edycji Professional, Enterprise oraz Ultimate - Windows 8 (32-bit oraz 64-bit) wszystkie edycje - Windows 8.1 (32-bit oraz 64-bit) wszystkie edycje - Windows 10 (32-bit oraz 64-bit) - Windows Server 2008 SP1 (32-bit) edycji Standard, Enterprise oraz Web Server - Windows Server 2008 SP1 (64-bit) edycji Standard, Enterprise, Web Server, Small Bussines Server oraz Essential Bussines Server - Windows Server 2008 R2 oraz Windows Server 2008 R2 SP1 edycji Standard, Enterprise oraz Web Server - Windows Server 2012 edycji Essentials, Standard oraz Datacenter - Windows Server 2012 R2 edycji Essentials, Standard oraz Datacenter - Windows Server 2016 edycji Essentials, Standard oraz Datacenter - Red Hat Enterprise Linux 5, 6 and 7 (32-bit oraz 64-bit) - CentOS 6, 7 (32-bit oraz b4-bit) - openSUSE 13.2 (32-bit oraz b4-bit) - SUSE Linux Enterprise Server 10 and 11 (32-bit oraz b4-bit) - SUSE Linux Enterprise Desktop 11 (32-bit oraz b4-bit) - Debian GNU Linux 7 and 8 (32-bit oraz b4-bit) - Ubuntu 12.04, 14.04, 16.04 (32-bit oraz b4-bit) 5. Możliwość instalacji konsoli zarządzania niezależnie na kilku wybranych stacjach. 6. Polski interfejs użytkownika i dokumentacja do oprogramowania na stację roboczą. Wymagania dotyczące technologii: 1. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanującego nośniki i monitora poczty elektronicznej, monitora ruchu http oraz moduł antyrootkitowy. 2. Co najmniej trzy różne silniki antywirusowe, funkcjonującejednocześnie i skanujące wszystkie dane. 3. Oddzielny silnik skanujący do wykrywania niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan". 4. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie. 5. Możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta. 6. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie. 7. Brak konieczności restartu komputerów po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów. 8. Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.

	9. Wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan", „rootkit". 10. Możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger", „dialer", „trojan" w kwarantannie. 11. Mechanizm centralnego zarządzania folderami kwarantanny znajdującymi się na stacjach klienckich. 12. Mechanizm skanujący wspólny dla wszystkich platform sprzętowych i programowych, wszystkich maszyn, wszystkich wersji oprogramowania, w tym bez względu na wersję językową oprogramowania – bez względu na to jak duża jest sieć lub jak bardzo jest złożona. 13. Mechanizm określania źródeł ataków prowadzonych przy użyciu zagrożeń hybrydowych. 14. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji). 15. Obsługa plików skompresowanych obejmująca najpopularniejsze formaty, w tym co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2. 16. Automatyczne usuwanie wirusów oraz oprogramowania typu malware i zgłaszanie alertów w przypadku wykrycia wirusa. 17. Logowanie historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów z poziomu GUI aplikacji. 18. Automatyczne uruchamianie procedur naprawczych. 19. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione. 20. Gwarancja na dostarczenie szczepionki na nowego wirusa w czasie krótszym niż 48 godzin. 21. Średni czas reakcji producenta na nowy wirus poniżej 8 godzin, 24 godziny na dobę przez cały rok (24/7/365). 22. Automatyczne powiadomienie użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem stacja robocza jest odpowiednio zabezpieczona. 23. Skanowanie przez program na komputerze klienckim przychodzącej i wychodzącej poczty elektronicznej bez konieczności instalowania dodatkowych programów/modułów. W programach pocztowych nie modyfikowane są ustawienia konta, tj. serwera POP3, SMTP i IMAP. Obsługuje m.in. MS Outlook Express, MS Outlook, Mozilla, Eudora, Netscape Mail. 24. Skanowanie przez program na komputerze klienckim, danych pobieranych i wysyłanych danych przy pomocy protokołu http. 25. Wsparcie dla technologii Cisco Network Admission Control (NAC). 26. Wsparcie dla technologii Microsoft Network Access Protection (NAP). 27. Ochrona przeglądarki internetowej, w tym: blokowanie wyskakujących okienek, blokowanie ciasteczek (cookies), blokowanie możliwości zmian ustawień w IE, analiza uruchamianych skryptów ActiveX i pobieranych plików. 28. Ochrona podczas przeglądania sieci Internet na podstawie badania reputacji – moduł działający na bazie Network Interceptor Framework (niezależnie od rodzaju i wersji przeglądarki). 29. Możliwość pobierania aktualizacji przez klientów między sobą – tzw. „Neighborcast" pozwalające na odciążenie łącza do sieci WAN.

	30. Ochrona rejestrów systemowych, w tym odpowiedzialnych za konfigurację przeglądarki Internet Explorer, listę uruchamianych aplikacji przy starcie, przypisania rozszerzeń plików do zadanych aplikacji. 31. Kontrola oraz możliwość blokowania aplikacji próbujących uzyskać połączenie z Internetem lub siecią lokalną. 32. Osobista zapora ogniowa (tzw. personal firewall) z możliwością definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup roboczych. 33. Moduł kontroli urządzeń zapewniający możliwość zezwolenia lub zabronienia dostępu do komputera urządzeń zewnętrznych (np. napędy usb, urządzenia bluetooth). 34. Moduł kontroli urządzeń zarządzany z poziomu konsoli centralnego zarządzania. 35. Moduł blokowania botnetów. 36. Moduł aktualizacji oprogramowania skanujący stacje robocze pod kontem niezastosowanych łatek systemu Windows i aplikacji firm trzecich oraz ich instalacji z poziomu konsoli centralnego zarządzania z możliwością definiowania wykluczeń trybu automatycznego na podstawie nazw programów lub identyfikatorów biuletynów. 37. Moduł kontroli zawartości internetowej umożliwiający ograniczenie dostępu do określonych usług i treści internetowych, a także pozwalający określić treści dostępne dla użytkowników. Wymagania dotyczące systemy zarządzania centralnego: 1. Konsola zarządzania umożliwia eksport pakietu instalacyjnego dla klienta w formacie Microsoft Installer (MSI) i JAR lub też bezpośrednią instalację zdalną nienadzorowaną. 2. Narzędzie instalacyjne musi sprawdzać istnienie poprzednich wersji oprogramowania. W przypadku znalezienia poprzedniej wersji instalator powinien pozostawić ustawienia użytkownika, usunąć starsze oprogramowanie z klienta lub serwera i instalować nowe wersję. 3. Pełna administracja konfiguracją i monitorowanie stacji roboczych i serwerów plików za pomocą konsoli administracyjnej (centralna instalacja, konfiguracja w czasie rzeczywistym, zarządzanie, raportowanie i administrowanie oprogramowaniem). 4. Komunikacja pomiędzy serwerem centralnego zarządzania a stacjami roboczymi musi być zaszyfrowana lub sygnowana stosownymi kluczami prywatnymi i publicznymi. 5. Scentralizowane blokowanie i odblokowywanie dostępu użytkownika do zmian konfiguracyjnych oprogramowania klienckiego, konsola pozwala na zdalne zarządzanie wszystkimi ustawieniami klienta. 6. Administratorzy muszą mieć możliwość tworzenia logicznych grup klientów i serwerów, w celu zarządzania oraz wymuszania określonych dla grupy zasad bezpieczeństwa. 7. Centralna konsola administracyjna musi umożliwiać przenoszenie klientów z jednej grupy do drugiej z możliwością zachowania ustawień lub dziedziczenia ustawień grupy. 8. Możliwość zmiany ustawień dla poszczególnych grup, umożliwienie administratorom zarządzania poszczególnymi klientami i funkcjonalnymi grupami klientów (tworzenie grup klientów). 9. Tworzenie grup, zdalne instalowanie oprogramowania oraz wymuszanie stosowania określonych zasad i ustawień na klientach. 10. Możliwość importu struktury drzewa z Microsoft Active Directory. 11. Możliwość blokowania wszystkich ustawień konfiguracyjnych stacji roboczych w celu uniemożliwienia ich modyfikacji przez użytkowników. 12. Serwer zarządzający związany z konsolą zarządzającą musi mieć funkcję przesyłania aktualizacji do klientów z możliwością ustawienia harmonogramu lub częstotliwości aktualizacji.

	13. Możliwość definiowania harmonogramów lub częstotliwości automatycznego pobierania aktualizacji definicji wirusów od producenta oprogramowania przez serwer zarządzający. 14. Możliwość instalacji i konfiguracji wewnętrznego serwera aktualizacji, łączącego się z serwerem aktualizacji producenta i aktualizacja serwerów, serwera zarządzającego oraz stacji roboczych z wewnętrznego serwera aktualizacji. 15. Możliwość ustalenia dodatkowego harmonogramu pobierania przez serwery plików i stacje robocze aktualizacji z serwera producenta. 16. Funkcja przechowywania i przekazywania danych umożliwiająca przechowywanie przez klientów danych dotyczących zdarzeń, w sytuacji, jeśli nie mogą oni uzyskać połączenia z serwerem zarządzania. 17. Dane powinny być przesyłane do serwera zarządzania podczas kolejnego połączenia. 18. Możliwość włączania/wyłączania wyświetlania komunikatów o znalezionych wirusach na wybranych stacjach klienckich. 19. Program musi pozwalać administratorowi zdefiniować treść komunikatu wyświetlanego w przypadku wykrycia wirusa. 20. Umożliwienie administratorom na audyt sieci, polegający na wykryciu niechronionych węzłów narażonych na ataki wirusowe. 21. Automatyczne wykrywanie i usuwanie oprogramowanie innych wiodących producentów systemów antywirusowych (min. 3 inne) podczas instalacji. 22. Automatyczne uaktualnianie bazy definicji wirusów oraz mechanizmów skanujących nie rzadziej niż co 7 dni (zalecane codzienne aktualizacje). 23. Automatyczne pobieranie przez program antywirusowy klienta zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe. 24. Możliwość eksportu raportów z pracy systemu do plikucsv i html. 25. Możliwość natychmiastowej aktualizacji przez serwer definicji wirusów na stacjach klienckich. 26. Możliwość uruchomienia aktualizacji stacji roboczych i serwerów przez użytkowników „na żądanie”. 27. Program musi pozwalać administratorowi na określenie reakcji w przypadku wykrycia wirusa. 28. Program musi pozwalać na określenie obszarów skanowania, tj.: pliki, katalogi, napędy lokalne i sieciowe. 29. Program musi pozwalać na skanowanie pojedynczych plików przez dodanie odpowiedniej opcji do menu kontekstowego (po kliknięciu prawym przyciskiem myszy). 30. Program musi pozwalać na określenie typów skanowanych plików, momentu ich skanowania (otwarcie, modyfikacja) oraz na wykluczenie ze skanowania określonych folderów. 31. Zarządzanie zdarzeniami i raportowanie – natychmiastowe alarmowanie o aktywności wirusów w administrowanej sieci na kilka sposobów: poczta elektroniczna, powiadomienia przez SNMP, raportowanie do dziennika systemowego, raportowanie do systemu centralnego zarządzania. 32. Możliwość tworzenia wielu kont dostępu do systemu centralnego zarządzania dla różnych użytkowników (w tym możliwość nadaniu danemu użytkownikowi ograniczonych praw).
Pakiet Biurowy	• Pakiet biurowy dostarczony wraz z licencją i nośnikiem. • Wymagania odnośnie interfejsu użytkownika: o Pełna polska wersja językowa interfejsu użytkownika.

	o Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych. o Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się. • Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: o posiada kompletny i publicznie dostępny opis formatu, o ma zdefiniowany układ informacji w postaci XML zgodnie z Tabelą B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2005.212.1766), o umożliwia wykorzystanie schematów XML, wspiera w swojej specyfikacji podpis elektroniczny zgodnie z Tabelą A.1.1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2005.212.1766) • Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców. • W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy), • Do aplikacji musi być dostępna pełna dokumentacja w języku polskim. • Pakiet zintegrowanych aplikacji biurowych musi zawierać: o Edytor tekstów o Arkusz kalkulacyjny o Narzędzie do przygotowywania i prowadzenia prezentacji o Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) • Edytor tekstów musi umożliwiać: o Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty. o Wstawianie oraz formatowanie tabel i obiektów graficznych. o Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne). o Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel, rysunków oraz tworzenie spisów treści. o Formatowanie nagłówków i stopek stron. o Sprawdzanie pisowni w języku polskim. o Śledzenie zmian wprowadzonych przez użytkowników. o Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. o Określenie układu strony (pionowa/pozioma). o Wydruk dokumentów. o Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.

	o Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003, 2007, 2010 i 2013 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów Dokumentu. o Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. o Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem. o Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa. o Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze pozwalające zapisać plik wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i Prawnych. • Arkusz kalkulacyjny musi umożliwiać: o Tworzenie raportów tabelarycznych i wykresów liniowych (wraz linią trendu), słupkowych, kołowych. o Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu. o Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice). o Obsługę „kostek OLAP” oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych. o Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych. o Wyszukiwanie i zamianę danych. o Wykonywanie analiz danych przy użyciu formatowania warunkowego. o Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie. o Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. o Formatowanie czasu, daty i wartości finansowych z polskim formatem. o Zapis wielu arkuszy kalkulacyjnych w jednym pliku. o Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003, 2007, 2010 i 2013 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń. o Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. • Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: o Przygotowywanie prezentacji multimedialnych, które będą: – Prezentowane przy użyciu projektora multimedialnego. – Drukowane w formacie umożliwiającym robienie notatek. – Zapisane jako prezentacja tylko do odczytu.

	o Nagrywanie narracji i dołączanie jej do prezentacji. o Opatrywanie slajdów notatkami dla prezentera. o Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo. o Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego. o Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym. o Możliwość tworzenia animacji obiektów i całych slajdów. o Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera. o Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, 2007 2010 i 2013. • Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: o Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego. o Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców. o Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną. o Automatyczne grupowanie poczty o tym samym tytule. o Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy. o Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia. o Zarządzanie kalendarzem. o Udostępnianie kalendarza innym użytkownikom. o Przeglądanie kalendarza innych użytkowników. o Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach. o Zarządzanie listą zadań. o Zlecanie zadań innym użytkownikom. o Zarządzanie listą kontaktów. o Udostępnianie listy kontaktów innym użytkownikom. o Przeglądanie listy kontaktów innych użytkowników. o Możliwość przesyłania kontaktów innym użytkowników.

1.3.5 ZARZĄDZALNY PRZEŁĄCZNIK – SWITCH

Switch

Nazwa komponentu	Wymagane minimalne parametry technicznych
Zarządzanie	Zarządzalny L2
Dostęp	Przeglądarka WWW (GUI) SNMP v1/v2c/v3 RMON
Architektura sieci	Gigabit Ethernet
Całkowita liczba portów	26
Rodzaje wejść wyjść	10/100/1000 Mbps - 24 szt. Combo port BASE-T/SFP - 2 szt.
Power over Ethernet (PoE)	PoE 802.3af (PSE) do 15.4W
Liczba portów PoE/PoE+	12
Obsługiwane protokoły	IEEE 802.3 IEEE 802.3u IEEE 802.3z IEEE 802.3ab IEEE 802.3ad IEEE 802.3az IEEE 802.3x IEEE 802.1d IEEE 802.1w IEEE 802.1q IEEE 802.1x IEEE 802.1p
Rozmiar tablicy MAC	8K
Gwarancja	Min. 3-letnia gwarancja (lub dłużej zgodnie ze złożoną ofertą), świadczona w miejscu instalacji. z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia.

1.3.6 KARTY ROZSZERZEŃ DO SERWERÓW I OPROGRAMOWANIE

Wykonawca ma obowiązek dostarczyć macierz o przedstawionych w kolejnym rozdziale minimalnych parametrach technicznych. Macierz musi współpracować (być w pełni kompatybilna) z serwerami będącymi na wyposażeniu Zamawiającego tj.: DELL POWEREDGE R510, DELL POWEREDGE R520 oraz DELL POWEREDGE R710.

W tym celu Wykonawca ma obowiązek (jeśli to konieczne) dostarczyć karty rozszerzeń do powyższych serwerów.

Konfiguracja posiadanych serwerów:

1) DELL POWEREDGE R510:
   - OS – Windows Server 2008 R2
   - Procesor: 2 x Intel(R) Xeon(R) CPU E5620 2.40GHz (łącznie 16 rdzeni)

- RAM: 24GB (6 x 4GB DDR3)
- HDD: SAS 8 x 300GB (skonfigurowane w RAID 1 i RAID 5)
- Zainstalowane role i funkcje: Serwery DNS, IIS, Usługi domenowe w usłudze Active Directory, Usługi plików
- Zainstalowane oprogramowanie serwerowe i bazodanowe: Apache Tomcat 8.0, Microsoft SQL Server 2012 Express, SQL Anywhere 9, Firebird SQL Server 2.5.

2) DELL POWEREDGE R520:
   - OS – Windows Server 2008 R2
   - Procesor: 1 x Intel(R) Xeon(R) CPU E5-2420 1.90GHz - 12 rdzeni
   - RAM: 16GB (2 x 8GB DDR3)
   - HDD: SAS 3 x 300GB, 5 x 600GB (skonfigurowane w RAID 1 i RAID 5)
   - Zainstalowane role i funkcje: Serwery DNS, DHCP, IIS, FTP, Usługi domenowe w usłudze Active Directory, Usługi plików i magazynowania
   - Zainstalowane oprogramowanie serwerowe i bazodanowe: PostgreSQL Server 8.4.
3) DELL POWEREDGE R710:
   - OS – Windows Server 2008 R2
   - Procesor: 2 x Intel(R) Xeon(R) CPU E5507 2.27GHz (łącznie 8 rdzeni)
   - RAM: 16GB (4 x 4GB DDR3)
   - HDD: SAS 2 x 146GB, 3 x 300GB (skonfigurowane w RAID 1 i RAID 5)
   - Zainstalowane role i funkcje: Serwery IIS, FTP, Usługi zasad i dostępu sieciowego
   - Zainstalowane oprogramowanie serwerowe i bazodanowe: Apache Tomcat7.0, Microsoft SQL Server 2005 Express, PostgreSQL Server 8.4.

Jednocześnie Zamawiający wymaga dostarczenia dla każdego z serwerów oprogramowania spełniającego poniższe wymagania minimalne:

1. Zainstalowany system musi umożliwiać obsługę co najmniej 32 GB pamięci RAM.
2. System musi automatycznie weryfikować cyfrowe sygnatury sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu.
3. System musi mieć możliwość dynamicznego obniżania poboru energii przez rdzenie procesora/ów nie wykorzystywane w bieżącej pracy.
4. System musi być wyposażony w mechanizmy klasyfikowania i indeksowania plików w oparciu o ich zawartość.
5. System musi umożliwiać uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
6. System musi umożliwiać automatyczną aktualizację w oparciu o poprawki publikowane przez producenta.
7. System musi umożliwiać zmianę języka interfejsu i posiadać minimum języki angielski i polski.
8. System musi być objęty polskojęzycznym cyklem szkoleń i zestawem materiałów szkoleniowych.
9. System musi posiadać polskojęzyczne wsparcie producenta systemu.
10. System musi mieć możliwość uruchomienia serwerów usług sieciowych takich jak WWW, DNS i DHCP.
11. System musi posiadać możliwość uruchomienia kontrolera usług katalogowych.
12. System musi umożliwiać pracę terminalową użytkownikom na zasadzie licencji dostępowych.

13. Jeżeli system, przy dostępie do zasobów serwera, wymaga licencji dostępowych, należy je dostarczyć dla 35 użytkowników. Zamawiający dysponuje odpowiednią liczbą licencji dostępowych dla systemu Windows Server 2012 R2, które mogą zostać wykorzystane.
14. System musi być dostarczony na nośniku instalacyjnym – płycie DVD.

1.3.7 MACIERZ DYSKOWA

MACIERZ

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Do instalacji w standardowej szafie RACK 19" rozwiązanie może zajmować maksymalnie 2U i pozwalać na instalacje 12 dysków 3.5"
Kontrolery	Dwa kontrolery RAID pracujące w układzie active-active posiadające łącznie minimum osiem portów SAS 12Gbps do podłączenia serwerów. Wraz z macierzą należy dostarczyć 3 kontrolery SAS 12Gb/s z portami wyprowadzonymi na zewnątrz oraz 6 kabli SAS 12Gb HD-Mini do HD-Mini o długości min. 0.5 metra.
Cache	4GB na kontroler, pamięć cache zapisu mirrorowana między kontrolerami, z opcją zapisu na dysk lub inna pamięć nieulotną lub podtrzymywana bateryjnie przez min. 72h w razie awarii
Dyski	Zainstalowane 9 dysków Hot-Plug SAS o pojemności 1.2TB SAS 12Gb/s 10k RPM, możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych do łącznie minimum 192 dysków, również dysków hot-plug typu SAS. Możliwość mieszania typów dysków w obrębie macierzy oraz pojedynczej półki.
Oprogramowanie	Zarządzające macierzą w tym powiadamianie mailem o awarii, umożliwiające maskowanie i mapowanie dysków. Licencja umożliwiającą utworzenie minimum 512 LUN'ów, 32 kopii migawkowych na LUN oraz kopię wirtualnych dysków. Licencja zaoferowanej macierzy powinna umożliwiać podłączanie minimum 4 hostów bez konieczności zakupu dodatkowych licencji. Zarządzanie macierzą poprzez minimum oprogramowanie zarządzające lub przeglądarkę internetową. Wymagana funkcja paska postępu – progressbar'u lub wyświetlenia wartości zaawansowania operacji w procentach przypadku formatowania wirtualnych dysków w oparciu o fizyczne dyski zainstalowane w macierzy. Dodatkowe oprogramowanie umożliwiające wspólne zarządzanie oferowanymi serwerami oraz oferowaną macierzą poprzez sieć spełniające minimalne wymagania: - Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych; - Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta; - Wsparcie dla protokołów– WMI, SNMP, IPMI, WSMan, Linux SSH; - Możliwość oskryptowywania procesu wykrywania urządzeń; - Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram; - Szczegółowy opis wykrytych systemów oraz ich komponentów; - Możliwość eksportu raportu do CSV, HTML, XLS; - Grupowanie urządzeń w oparciu o kryteria użytkownika; - Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach; - Automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń; - Szybki podgląd stanu środowiska; - Podsumowanie stanu dla każdego urządzenia; - Szczegółowy status urządzenia/elementu/komponentu; - Generowanie alertów przy zmianie stanu urządzenia;

	- Filtry raportów umożliwiające podgląd najważniejszych zdarzeń; - Integracja z service desk producenta dostarczonej platformy sprzętowej; - Możliwość przejęcia zdalnego pulpitu; - Możliwość podmontowania wirtualnego napędu; - Automatyczne zaplanowanie akcji dla poszczególnych alertów w tym automatyczne tworzenie zgłoszeń serwisowych w oparciu o standardy przyjęte przez producentów oferowanego w tym postępowaniu sprzętu; - Kreator umożliwiający dostosowanie akcji dla wybranych alertów; - Możliwość importu plików MIB ; - Przesyłanie alertów „as-is" do innych konsol firm trzecich; - Możliwość definiowania ról administratorów ; - Możliwość zdalnej aktualizacji sterowników i oprogramowania wewnętrznego serwerów; - Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) - Możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta - Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów - Możliwość wykorzystania dysków SSD jako cache macierzy, jeśli dla tej funkcjonalności jest wymagana licencja należy uwzględnić licencję wraz z macierzą. - Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych
Wsparcie dla systemów operacyjnych	Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 SP1, Red Hat Enterprise Linux (RHEL),Microsoft Windows 2003 SP2 and R2, Microsoft Windows Storage Server 2003 R2 and SP2, VMware ESX 3.5; 4; 4.1; 5, XenServer Express Edition
Bezpieczeństwo	Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne.
Warunki gwarancji dla macierzy	Min. 3-letnia gwarancja (trzy letnia lub dłużej zgodnie ze złożoną ofertą), świadczona na miejscu u klienta, czas reakcji serwisu - do końca następnego dnia roboczego. W przypadku awarii dysków twardych, dysk pozostaje u Zamawiającego bez dodatkowych opłat. Możliwość rozszerzenia gwarancji przez producenta do 7 lat. • Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji macierzy. • Wszystkie naprawy gwarancyjne powinny być możliwe na miejscu. • Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części I transportu. • W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
Certyfikaty	Macierz musi być wyprodukowana zgodnie z normą ISO 9001 lub równoważną.

1.3.8 LASEROWE URZĄDZENIE WIELOFUNKCYJNE A3

Urządzenie wielofunkcyjne kolorowe A3 (drukarka, skaner, kopiarka, fax) – 1 szt

	Minimalne parametry
Drukowanie	
Szybkość drukowania w mono	A4: 23 str./min; A3: 13 str./min
Szybkość drukowania w kolorze	A4: 23 str./min; A3: 13 str./min
Czas pierwszego wydruku	14 sekund
Rozdzielczość	1200 x 600 dpi
Języki druku	PCL5c, PCL6, emulacja PostScript3, XPS, PDF (v1.7)
Zespół drukowania	Dupleks mechaniczny
Skanowanie	
Rozdzielczość skanowania	600 x 600 dpi
Szybkość skanowania	50 str./min
Podawanie dokumentów	Automatyczny podajnik dokumentów wraz z duplexem na 100 arkuszy, skaner płaski
Format skanowania	TIFF, PDF, XPS, JPEG
Książka adresowa	LDAP i wewnętrzna książka adresowa
Skanowanie do	FTP, HTTP, E-mail, CIFS, pamięci USB, skanowanie zdalne
Kopiowanie	
Czas wykonania pierwszej kopii	15 sekund w kolorze/ czarno-białym
Szybkość kopiowania	do 23 kopii/min w kolorze oraz czarno-białym
Rozdzielczość kopiowania	300/600dpi
Zmniejszanie/powiększanie	Zoom 25-400%
Faksowanie	
Złącza	RJ11 x 2 (Line/Tel), PSTN, Linia PBX
Szybkość	ITU-T G3(Super G3) do 33,6kbps,
Pamięć stron	8 MB
Interfejs i oprogramowanie	
Złącza	Port USB 2.0, Ethernet 10/100/1000 BaseTX, Host USB x 2, sieć bezprzewodowa 802.11a/b/g/n (opcjonalnie)
Kompatybilność z systemami operacyjnymi	tak
Zaawansowane funkcje sieci oraz bezpieczeństwo	Filtrowanie IP, filtrowanie MAC, SSL/TLS, EAP(IEEE802.1X), IPSec
Dodatkowe oprogramowanie	Oprogramowanie producenta drukarki lub równoważne do monitorowania wykorzystania urządzenia oraz nakładania ograniczeń posiadające następujące funkcje: • funkcjonować w środowisku Windows; • obsługiwać zarówno drukarki sieciowe (czyli podłączone do sieci Ethernet poprzez wbudowaną w drukarkę wewnętrzną kartę sieciową) jak i drukarki podłączone lokalnie (przez port USB i/lub LPT) • podawać nazwy użytkowników (np. ich loginy) drukujących poszczególne wydruki; • podawać nazwy drukowanych plików, liczbę stron, datę i godzinę przeprowadzenia danego wydruku;

	• możliwość wpisania kosztów materiałów eksploatacyjnych, oraz kosztu użycia zwykłej kartki, folii i nalepek; • podawać koszt przeprowadzonego wydruku z możliwością rozróżnienia wydruków o małym i dużym pokryciu (wymagane jest rozróżnianie przynajmniej 5 różnych poziomów pokrycia, i przyznawanie im odpowiednich kosztów); • w przypadku nakładania ograniczeń, powinien umożliwiać blokadę druku kolorowego z jednoczesną możliwością automatycznej konwersji tych plików na postać czarno-białą która byłaby wykonywana na drukarce; • możliwość nakładania ograniczeń ilościowych na liczbę drukowanych stron oraz na koszty wydruku, w ujęciu dziennym, tygodniowym i miesięcznym.
Podawanie papieru	
Pojemność papieru	Podajnik 1: 300 arkuszy 80 g/m2; Podajnik 2: 535 arkuszy 80 g/m2 wyposażony w zintegrowaną szafkę na kółkach Podajnik wielofunkcyjny: 100 arkuszy 80 g/m2; Podajnik RADF: 100 arkuszy 80 g/m2;
Format papieru	A3, A4, B4, A5, B5, A6
Gramatura papieru	64 – 256 g/m2
Odbiornik papieru	Do 250 arkuszy na dolnej tacy, 100 arkuszy na górnej tacy
Dodatkowe wyposażenie	Urządzenie wyposażone w zszywacz zewnętrzny stanowiący integralną część urządzenia umożliwiający zszywanie min. 20 arkuszy 80 g/m2;
Przebieg papieru	Płaski przebieg przy materiałach o dużej gramaturze
Pozostałe parametry techniczne:	
Pamięć (RAM)	Standardowa pamięć RAM: 1,26 GB
Panel	7-calowy (17,5cm) podświetlany kolorowy ekran dotykowy
Szybkość procesora	800 MHz
Dysk twardy	dysk twardy o minimalnej pojemności 250 GB
Obciążenie	Maksymalne obciążenie do 60 000 stron miesięcznie
Wymaganie dodatkowe:	
Gwarancja	Min. 3-letnia gwarancja (trzy letnia lub dłużej zgodnie ze złożoną ofertą), świadczona na miejscu u klienta, czas reakcji serwisu - do końca następnego dnia roboczego. - naprawa w miejscu instalacji w ciągu 24h od daty zgłoszenia lub sprzęt zastępczy.

1.3.9 LASEROWE URZĄDZENIE WIELOFUNKCYJNE A4

Urządzenie wielofunkcyjne monochromatyczne A4 (drukarka, skaner, kopiarka, fax) – 1szt.

	Minimalne parametry
Drukowanie	
Szybkość drukowania	33 str./min
Szybkość druku dwustronnego	18 str/min
Czas pierwszego wydruku	6,5 sekund
Rozdzielczość	1200 x 1200 dpi
Języki druku	PCL5e, PCL6, IBM-PPR, Epxon-FX,XPS

Zespół drukowania	Dupleks mechaniczny
Skanowanie	
Rozdzielczość skanowania	600 x 600 dpi
Szybkość skanowania	Do 6 s/stronę w kolorze, 2s/stronę w czerni
Głębia kolorów	Wejście 48 bit/Wyjście 24 bit
Podawanie dokumentów	Automatyczny podajnik dokumentów wraz z duplexem na 50 arkuszy, skaner płaski
Format	M-TIFF, PDF, XPS, JPEG, GIF, PNG
Książka adresowa	LDAP, 300 adresów e-mail, 20 grup adresowych
Skanowanie do	FTP, HTTP, E-mail, TWAIN, CIFS, pamięci USB,
Kopiowanie	
Czas wykonania pierwszej kopii	10 sekund
Szybkość kopiowania	do 33 kopii/min
Rozdzielczość kopiowania	do 600 x 600dpi
Zmniejszanie/powiększanie	Zoom 25-400%
Maksymalna liczba kopii	99
Faksowanie	
Złącza	RJ11 x 2 (Line/Tel), PSTN, Linia PBX
Szybkość	ITU-T G3(Super G3) do 33,6kbps, do 2 s/str.
Szybkie wybieranie	16 przycisków szybkiego wybierania, 300 numerów
Lista rozgłaszania	Maksimum 100
Pamięć stron	4MB
Interfejs i oprogramowanie	
Złącza	Port USB 2.0, Ethernet 10/100/1000BaseTX
Komunikacja bezprzewodowa	Tak, moduł bezprzewodowej karty sieciowej wbudowanej w urządzenie.
Kompatybilność z systemami operacyjnymi	Windows XP (32-bit & 64-bit) / Server 2003 (32-bit & 64-bit) / Server 2008 (32-bit & 64-bit) / Server 2008 R2 (64-bit) / Vista (32-bit & 64-bit) / 7 (32-bit & 64-bit); Linux PPD, Mac OS X 10.6.8 - 10.7, 10.8, 10.9
Dodatkowe oprogramowanie	Oprogramowanie producenta drukarki lub równoważne do monitorowania wykorzystania urządzenia oraz nakładania ograniczeń posiadające następujące funkcje: - funkcjonować w środowisku Windows; - obsługiwać zarówno drukarki sieciowe (czyli podłączone do sieci Ethernet poprzez wbudowaną w drukarkę wewnętrzną kartę sieciową) jak i drukarki podłączone lokalnie (przez port USB i/lub LPT) - podawać nazwy użytkowników (np. ich loginy) drukujących poszczególne wydruki; - podawać nazwy drukowanych plików, liczbę stron, datę i godzinę przeprowadzenia danego wydruku; - możliwość wpisania kosztów materiałów eksploatacyjnych, oraz kosztu użycia zwykłej kartki, folii i nalepek; - podawać koszt przeprowadzonego wydruku z możliwością rozróżnienia wydruków o małym i dużym pokryciu (wymagane jest rozróżnianie przynajmniej 5 różnych poziomów pokrycia, i przyznawanie im odpowiednich kosztów); - możliwość nakładania ograniczeń ilościowych na liczbę drukowanych stron oraz na koszty wydruku, w ujęciu dziennym, tygodniowym i miesięcznym.

Podawanie papieru	
Pojemność papieru	Podajnik 1: 250 arkuszy 80 g/m2; Podajnik uniwersalny: 100 arkuszy 80 g/m2; Możliwość instalacji dodatkowego podajnika papieru o pojemności 530 arkuszy 80g/m2
Format papieru	Podajnik 1: A4, A5, B5, A6 Podajnik uniwersalny: A4, A5, B5, A6, Monarch, Com-9, Com-10, DL, C5, C6, Druk dwustronny: A4, B5
Gramatura papieru	Podajnik 1: 60 – 120 g/m2; Druk dwustronny: 60 – 120 g/m2; Podajnik uniwersalny: 60 – 120 g/m2 Podajnik skanera: 60 – 105 g/m2
Odbiornik papieru	Do 150 arkuszy stroną zadrukowaną do dołu
Pozostałe parametry techniczne:	
Pamięć (RAM)	Standardowa pamięć RAM: 512 MB
Obciążenie	Maksymalne obciążenie do 60 000 stron miesięcznie
Wymaganie dodatkowe:	
Gwarancja	Min. 3-letnia gwarancja (trzy letnia lub dłużej zgodnie ze złożoną ofertą), świadczona na miejscu u klienta, czas reakcji serwisu - do końca następnego dnia roboczego. - naprawa w miejscu instalacji w ciągu 24h od daty zgłoszenia lub sprzęt zastępczy.
Materiały eksploatacyjne:	Wymagana rozdzielność bębna i tonera. Toner startowy na 2 tys stron zgodnie z normą ISO/ISC 19752 Urządzenie dostarczone musi być fabrycznie nowe, skonfigurowane, gotowe do pracy wraz z tonerem(-ami) umożliwiającym wydruk przynajmniej 7 000 stron A4 przy pokryciu zgodnie z normą ISO/ISC 19752. Toner musi być tego samego producenta co drukarka, nie mogą być regenerowane.

1.3.10 DRUKARKA KODÓW KRESKOWYCH WSPÓŁPRACUJĄCA Z EZD

Drukarka – 1szt.

	Minimalne parametry
Drukowanie	
Metoda druku	d – termiczna, t - termotransferowa
Szybkość druku	127mm/sek.
Rozdzielczość	203dpi
Max. szer. druku	104mm
Max szer. etykiety	108mm
Max. długość druku	991mm
Orientacja druku	0°, 90°, 180°, 270°
Nawój taśmy ttr.	74m, zewnętrzny
Pamięć wbudowana	FLASH 4MB, SDRAM 8MB standardowo
Komunikacja	Standardowo podwójny interfejs: szeregowy RS-232, DB-9 i USB 1.1, dwukierunkowy, 10/100 Ethernet (opcja zamiast szeregowego)

Fonty wbudowane	16 bitmapowych ZPLII, 1czcionka skalowalna ZPL, 5 czcionek rozszerzalnych EPL2; wbudowana obsługa czcionek OpenTypeTM
Sterowniki	Win 9x /Me/ NT v.4.0, XP, w zestawie
Język programowania	EPL i ZPL standardowo
Drukowane kody	1D:Codabar, Code 11(ZPL), Code 39, Code 93, Code 128, EAN-8, EAN-13, EAN-14 (ZPL), German Post Code (EPL), GS1 DataBar (RSS), Industrial 2-of-5 (ZPL), Interleaved 2-of-5, ISBT-128 (ZPL), JapanesePostnet (EPL), Logmars (ZPL), MS1, Plessey, Postnet, standard 2-of-5 (ZPL), UCC/EAN-128(EPL), UPC-A, UPC-A I UPC-E z rozszerzeniami 2- lub 5-cyfrowymi EAN, UPC-E, UPC i rozszerzenia 2- lub 5-cyfrowe EAN (ZPL) 2D:Codablock (ZPl), Code 49 (ZPL), Data Patrix, (ZL), MaxiCode, MicroPDF417, PDF417, QR Code
Temperatura pracy	4,4°C - 41°C
Zasilanie	100-240V, 50-60 Hz
Opcje	10/100 Ethernet
Głowica drukująca	Gwarancja producenta: 6 miesięcy. Wymiana następuje w wypadku fizycznego starcia lub przepalenia punktu grzewczego. Głowice nie podlegają regeneracji.

Dokument podpisany elektronicznie

Dokument podpisany przez Jadwiga Zawadzka
Data: 2017.03.21 15:13:58 CET