

Lp.	Typ przedmiotu	Wymagane minimalne parametry techniczne przedmiotu	Ilość
CZĘŚĆ I – Sprzęt komputerowy, oprogramowanie, drukarki, oraz sprzęt multimedialny.			
1	Zestaw komputerowy (Typ A)	<p>Typ: Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta.</p> <p>Zastosowanie: Komputer będzie wykorzystywany do kształcenia na kierunku technik informatyk, aplikacji edukacyjnych, aplikacji obliczeniowych, aplikacji sieciowych, aplikacji serwerowych, tworzenia grafik 2D i 3D oraz renderingu wideo, wirtualizacji systemów operacyjnych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna.</p> <p>Wydajność obliczeniowa: Procesor klasy x86–ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach stacjonarnych, taktowany zegarem co najmniej 2,8 GHz, pamięcią last level cache CPU co najmniej 9MB, lub równoważny. Procesor powinien osiągać w teście wydajności PassMark PerformanceTest (wynik dostępny: http://www.passmark.com/products/pt.htm) co najmniej wynik minimum 11500 punktów Passmark CPU Mark – Załącznik Nr 8 do SIWZ</p> <p>Zamawiający zastrzega sobie, że w celu sprawdzenia poprawności przeprowadzenia testu Oferent musi udostępnić Zamawiającemu licencjonowane oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego.</p> <p>Pamięć operacyjna: min. 16 GB-DDR4 2666 MHz możliwość rozbudowy do min. 32 GB, minimum jeden slot wolny na dalszą rozbudowę pamięci.</p> <p>Parametry pamięci masowej: Wewnętrzny dysk twardy SSD o pojemności min. 256 GB, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii bez dodatkowych nośników.</p> <p>Wydajność grafiki: zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki, ze wsparciem dla DirectX 12, OpenGL 4.5, osiągająca min. 1190 pkt w teście Videocard Benchmark (http://www.videocardbenchmark.net/) – Załącznik Nr 9 do SIWZ</p> <p>Wypożyczenie multimedialne: Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, porty słuchawek i mikrofonu na przednim oraz na tylnym panelu obudowy, obudowa wyposażona w głośnik.</p> <p>Obudowa i zasilacz:</p> <p>Obudowa przystosowana do pracy w pionie.</p> <p>Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż pojedynczego dysku twardego 3,5 cala, napędu optycznego, kart rozszerzeń oraz obudowy.</p>	16

		<p>Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki).</p> <p>Obudowa musi być wyposażona w głośnik.</p> <p>Obudowa musi być wyposażona w zamek na klucz chroniący dostęp do wnętrza komputera – zamek nie może wystawiać poza obrys obudowy komputera.</p> <p>Obudowa musi być wyposażona w czujnik otwarcia obudowy współpracujący z oprogramowaniem diagnostyczno-monitorującym producenta komputera. Po aktywacji czujnika zdarzenie otwarcia obudowy musi być rejestrowane w logu dostępnym w ustawieniach BIOS komputera.</p> <p>Obudowa typu mini tower z obsługą kart PCI Express wyłącznie o pełnym profilu, wyposażona w min. 5 kieszeni: min. 2 szt. 5,25" zewnętrzne (dopuszcza się maksymalnie jedną zatokę na napęd optyczny typu SLIM), min. 1 szt. 3,5" wewnętrzne, min. 1 szt. 3,5" zewnętrzna.</p> <p>W celu szybkiej weryfikacji usterki w obudowę komputera musi być wbudowany akustyczny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami.</p> <p>Obudowa musi być wyposażona w pokrywę chroniącą gniazda na tylnej ścianie komputera przed niepowołanym dostępem i przed przypadkowym wypięciem kabli zamykana za pomocą zamka blokującego dostęp do wnętrza komputera.</p> <p>Zasilacz o mocy minimum 280W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 94%, przy 50% obciążeniu - wymagane jest dostarczenie karty katalogowej produktu potwierdzające te parametry. Suma wymiarów obudowy (wysokość + szerokość + głębokość mierzona po krawędziach zewnętrznych) nie może wynosić więcej niż 860 mm.</p> <p>BIOS</p> <ul style="list-style-type: none"> • Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: <ul style="list-style-type: none"> ○ Modelu komputera ○ Numerze seryjnym ○ wersji BIOS, ○ dacie produkcji BIOS, ○ ilości, częstotliwości taktowania i sposobu obłożenia kanałów pamięciami RAM, ○ modelu płyty głównej ○ nazwie komputera ○ typie procesora wraz z informacją o częstotliwości taktowania ○ producencie, modelu oraz pojemności zainstalowanego dysku twardego ○ MAC adresie zintegrowanej karty sieciowej 	
--	--	---	--

		<ul style="list-style-type: none"> • Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS) • Możliwość z poziomu BIOS-u włączenia/wyłączenia funkcji automatycznej aktualizacji BIOS-u. System powinien umożliwiać zdefiniowanie adresu IP serwera TFTP w sieci lokalnej lub podanie nazwy serwera, w którego bezpośrednio z poziomu BIOS-u można dokonać aktualizacji BIOS-u. System powinien umożliwiać również określenie częstotliwości sprawdzania dostępności nowszej wersji BIOS-u z częstotliwością co najmniej: raz dziennie, raz na tydzień, raz na miesiąc i raz na kwartał. • Możliwości aktualizacji BIOS-u w tym co najmniej: całkowite wyłączenie możliwości aktualizacji, możliwość aktualizacji za pomocą narzędzi producenta komputera lub mechanizmu Windows Update, możliwość aktualizacji jedynie za pomocą narzędzi producenta komputera • Możliwość włączania/wyłączania sprzętowego wsparcia wirtualizacji w procesorze liczby aktywnych rdzeni procesora; • Możliwość włączania/wyłączania technologii SpeedStep oraz Turbo • Możliwość wyboru trybu pracy systemu chłodzenia komputera spośród co najmniej w trzech ustawień: automatyczny, maksymalna wydajność CPU oraz maksymalna prędkość wentylatorów. • Możliwość monitorowania temperatury rdzenia procesora, obudowy procesora oraz temperatury wewnątrz obudowy komputera oraz prędkości obrotowej wentylatora. • Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznymi urządzeniami • Możliwość ustawienia trybu pracy komputera po przywróceniu zasilania po awarii zasilania w co najmniej trzech trybach: pozostaje wyłączony, zawsze wyłączony, zawsze włączony, przywrócenie stanu z przed awarii • 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 (dla wszystkich rodzajów dysków twardych w tym dysków M.2). • Możliwość ustawienia poziomu zabezpieczenia BIOS-u za pomocą hasła co najmniej na dwóch poziomach: • Standardowy: umożliwiający skasowanie hasła za pomocą zworki na płycie głównej 	
--	--	---	--

		<ul style="list-style-type: none"> • Silny: umożliwiający zresetowanie hasła jedynie poprzez interwencję serwisu • Możliwość włączenia/wyłączenia zintegrowanej karty dźwiękowej, karty sieciowej, modułu TPM z poziomu BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. • Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. • Możliwość wyłączenia portów USB w tym: wszystkich portów, tylko portów znajdujących się na przedzie obudowy, tylko tylnych portów, tylko zewnętrznych, wszystkich nieużywanych. W przypadku włączenia jedynie przednich lub jedynie tylnych lub jedynie używanych portów wymagana jest możliwość określenia czy włączone mają być jedynie porty USB do których podłączona jest klawiatura i mysz lub możliwość wyłączenia portów do których podłączone są pamięci masowe lub hub USB. <p>Dodatkowe oprogramowanie</p> <p>Oprogramowanie dostarczone przez producenta komputera pozwalające na zdalną inwentaryzację komputerów w sieci, lokalną i zdalną inwentaryzację komponentów komputera, umożliwiające co najmniej:</p> <ul style="list-style-type: none"> • Informowanie administratora o otwarciu obudowy • Zdalne wyłączenie, restart oraz hibernacje komputera w sieci, • Tworzenie raportów stanu jednostki, • Monitorowanie stanu komponentów: CPU, Pamięć RAM, HDD, wersje BIOS, • Aktualizację BIOS do najnowszej wersji zarówno dla pojedynczej maszyny jak i grupy, • Tworzenie kopii zapasowych BIOS wraz z ustawieniami • Tworzenie indywidualnych numerów dla poszczególnych użytkowników, • Włączenie lub wyłączenie BOOTowania portów USB • W pełni automatyczną instalację sterowników urządzeń opartą o automatyczną detekcję posiadanego sprzętu. <p>Certyfikowane oprogramowanie umożliwiające w bezpieczny (bezpowrotny) sposób usunięcie danych z dysku twardego z poziomu BIOS-u bez względu na stań czy obecność systemu operacyjnego – w ofercie należy podać nazwę oprogramowania oraz producenta.</p> <p>Wymagania dodatkowe:</p> <ul style="list-style-type: none"> • Wbudowane porty minimalnie: <ul style="list-style-type: none"> – 1 x DVI-D – 1 x Display Port 1.2 	
--	--	--	--

		<ul style="list-style-type: none"> – 1 x eSATA – 1 x RJ-45 – 1 x Czytnik kart pamięci z przodu obudowy – 1 x Audio: line-in – 1 x Audio: line-out – 1 x Audio: mikrofon z przodu obudowy – 1 x Audio: słuchawki z przodu obudowy – 8 szt. USB w tym: minimum 4 porty z przodu obudowy (w tym min. 2 x USB 3.0), minimum 4 porty z tyłu obudowy (w tym min. 2 x USB 3.0. Porty te powinny być wlutowane w płytę główną – nie dopuszcza się portów wyprowadzonych z płyty głównej na zewnątrz komputera za pomocą przewodów, taśm itp. <p>Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.</p> <ul style="list-style-type: none"> • Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika) • 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 (TPM co najmniej w wersji 2.0) • Płyta główna z wbudowanymi: <ul style="list-style-type: none"> – 1 złącze PCI-Express 2.0 x4 (mech. x16) – 1 złącze PCI-Express 3.0 x16 – 1 złącze M.2-2280 umożliwiające zamontowanie modułu SSD NVMe (PCI-Express 2.0) • Minimum 2 złącza DIMM z obsługą do 32GB DDR4 pamięci RAM, min. 3 złącz SATA 3.0 NCQ, min. 1x złącze m.2 2280, płyta musi być trwale oznaczona logo producenta komputera • Klawiatura w układzie QWERTY US • Mysz przewodowa z trzema klawiszami oraz rolką (scroll) min. 1000 dpi • Wewnętrzna nagrywarka DVD +/-RW <p>Normy i standardy</p> <p>Komputery mają spełniać normy i posiadać deklaracje zgodności (lub inne dokumenty potwierdzające spełnienie norm) w zakresie:</p> <ul style="list-style-type: none"> • Deklaracja zgodności CE • normy Energy Star 7.0 	
--	--	--	--

		<ul style="list-style-type: none"> • Certyfikat EPEAT na poziomie GOLD dla Polski - wymagany wpis dotyczący oferowanego modelu komputera w internetowym katalogu http://www.epeat.net - dopuszcza się wydruk ze strony internetowej • Być wykonane/wyprodukowane w systemie zapewnienia jakości ISO 9001/14001 Wymienione wyżej normy i deklaracje jakości mogą być zastąpione normami i deklaracjami jakości równoważnymi. Wykonawca będzie miał obowiązek wykazania, że wskazane normy i deklaracje równoważne zapewniają tę samą jakość i bezpieczeństwo dostarczonych komputerów, co normy i deklaracje wskazane przez Zamawiającego. <p>Zamawiający wymaga:</p> <ul style="list-style-type: none"> • dla potwierdzenia, że oferowany sprzęt odpowiada postawionym wymaganiom i był wykonany przez Wykonawcę (a jeżeli Wykonawca nie jest producentem to przez producenta) w systemie zapewnienia jakości wg normy ISO 9001 aby Wykonawca posiadał: Certyfikat ISO 9001 lub inne zaświadczenie/dokument wydane przez niezależny podmiot zajmujący się poświadczaniem zgodności działań wykonawcy z normami jakościowymi odpowiadającej normie ISO 9001 (załączyć dokument potwierdzający spełnianie wymogu). • Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia wykonawcy wystawionego na podstawie dokumentacji producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram. • Gwarancja jakości producenta: <ul style="list-style-type: none"> ○ Na okres co najmniej 36 miesięcy - świadczonej w siedzibie Zamawiającego, chyba że niezbędne będzie naprawa sprzętu w siedzibie producenta lub autoryzowanym przez niego punkcie serwisowym - wówczas koszt transportu do i z naprawy pokrywa Wykonawca, ○ Czas reakcji na zgłoszoną reklamację gwarancyjną - do końca następnego dnia roboczego ○ Naprawy gwarancyjne urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta, 	
--	--	---	--

		<ul style="list-style-type: none"> • Wsparcie techniczne producenta <ul style="list-style-type: none"> ○ 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 – do oferty należy dołączyć link strony. <p>System operacyjny: Microsoft Windows 10 Professional PL lub równoważny.</p> <p>Opis równoważności:</p> <p>Nie wymagający aktywacji za pomocą Internetu lub telefonu.</p> <p>Zainstalowany system operacyjny, w polskiej wersji językowej.</p> <p>Dołączony nośnik optyczny (CD/DVD) z instalatorem systemu operacyjnego oraz wszystkimi niezbędnymi do poprawnej pracy zestawu komputerowego sterownikami – parametry techniczne i funkcjonalne systemu.</p> <p>System operacyjny klasy desktop, 64-bit.</p> <p>Dostępne dwa rodzaje graficznego interfejsu użytkownika poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji, w tym:</p> <ol style="list-style-type: none"> 1) klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy; 2) dotykowy umożliwiający sterowanie dotykaniem na urządzeniach typu tablet lub monitorach dotykowych. <p>Interfejsy użytkownika dostępne w wielu językach do wyboru, w tym:</p> <ol style="list-style-type: none"> 1) polskim; 2) angielskim. <p>Zlokalizowane w języku polskim, co najmniej następujące elementy:</p> <ol style="list-style-type: none"> 1) menu; 2) odtwarzacz multimedialny; 3) pomoc; 4) komunikaty systemowe. <p>Wbudowany system pomocy w języku polskim.</p> <p>Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim.</p> <p>Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modulem „uczenia się” pisma użytkownika – obsługa języka polskiego.</p> <p>Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modulem „uczenia się” głosu użytkownika.</p> <p>Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne.</p>	
--	--	--	--

	<p>Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.</p> <p>Wbudowana zaporą internetowa (firewall) dla ochrony połączeń internetowych.</p> <p>Zintegrowana z systemem operacyjnym konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.</p> <p>Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.</p> <p>Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi).</p> <p>Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer.</p> <p>Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji.</p> <p>Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji.</p> <p>Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe.</p> <p>Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie.</p> <p>Możliwość pracy systemu w trybie ochrony kont użytkowników.</p> <p>Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu.</p> <p>Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów, w tym:</p> <ol style="list-style-type: none"> 1) poziom menu; 2) poziom otwartego okna systemu operacyjnego. <p>Wbudowany system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych.</p> <p>Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.</p> <p>Obsługa standardu NFC (near field communication).</p> <p>Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).</p> <p>Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.</p> <p>Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.</p> <p>Mechanizmy logowania do domeny w oparciu o:</p> <ol style="list-style-type: none"> 1) login i hasło; 2) karty z certyfikatami (smartcard); 	
--	---	--

	<p>3) wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).</p> <p>Mechanizmy wieloelementowego uwierzytelniania.</p> <p>Wsparcie dla uwierzytelniania na bazie Kerberos v. 5.</p> <p>Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu.</p> <p>Wsparcie dla algorytmów Suite B (RFC 4869).</p> <p>Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec.</p> <p>Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk.</p> <p>Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.</p> <p>Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń.</p> <p>Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.</p> <p>Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową.</p> <p>Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację.</p> <p>Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający niezawodność i pozwalający tworzyć kopie zapasowe.</p> <p>Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.</p> <p>Udostępnianie modemu.</p> <p>Wbudowane oprogramowanie do tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.</p> <p>Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.</p> <p>Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).</p> <p>Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).</p> <p>Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych.</p>	
--	--	--

	<p>Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika.</p> <p>Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w układzie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB.</p> <p>Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych.</p> <p>Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.</p> <p>Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.</p> <p>Do każdego zestawu komputerowego dostarczony monitor:</p> <p>Typ ekranu: Panoramiczny; ciekłokrystaliczny z aktywną matrycą IPS 24" (nie mniej niż 23,8 cala), utwardzany (3H);</p> <p>Jasność: min. 250 cd/m²</p> <p>Możliwość obrotu (Swivel): min. 340°;</p> <p>Pivot: tak</p> <p>Kontrast: min. 1000:1</p> <p>Wielkość plamki (maks): 0,2745 mm</p> <p>Kąty widzenia (pion/poziom): min. 178°/178° (CR10:1)</p> <p>Czas reakcji matrycy: max 5 ms</p> <p>Możliwość zmiany wysokości (min.): 15 cm</p> <p>Kolory: min. 16,7 mln</p> <p>Rozdzielczość maksymalna: 1920 x 1080 pikseli</p> <p>Powłoka powierzchni ekranu: Przeciwodblaskowa, utwardzona (3H)</p> <p>Zakres pochylenia monitora (min.): Od -5° do +35°</p> <p>Złącze (min): 15-stykowe złącze D-Sub, DVI-D (z HDCP), HDMI</p> <p>Średnie użycie energii (maks.): 15 W</p> <p>Inne: Monitor musi posiadać usuwalną podstawę montażową, wbudowane min. 2 głośniki min. 2W, oraz hub USB min. 2x USB 2.0; kompatybilność z VESA 100 mm, Kensington Lock</p> <p>Dołączone oprogramowanie producenta monitora pozwalające na zdalne sprawdzenie parametrów pracy oraz konfigurację ustawień monitora</p> <p>Normy i standardy: Monitory muszą być wykonane zgodnie normami i posiadać certyfikaty: TCO 7.0, ISO9241-307, EPEAT Gold, Energy Star 7.0, TÜV Low Blue Light, TÜV Flicker Free – lub inne dokumenty wdane przez niezależny podmiot uprawniony do kontroli jakości, potwierdzające, że dostarczone monitory odpowiadają wskazanym normom.</p> <p>Wymienione wyżej normy i deklaracje jakości mogą być zastąpione normami i deklaracjami jakości równoważnymi. Wykonawca będzie miał obowiązek wykazania, że wskazane normy i deklaracje równoważne</p>	
--	---	--

		<p>zapewniają tę samą jakość i bezpieczeństwo dostarczonych komputerów, co normy i deklaracje wskazane przez Zamawiającego.</p> <p>Gwarancji jakości producenta:</p> <ul style="list-style-type: none"> • Na okres co najmniej 36 miesięcy - świadczonej w siedzibie Zamawiającego, chyba że niezbędne będzie naprawa sprzętu w siedzibie producenta lub autoryzowanym przez niego punkcie serwisowym - wówczas koszt transportu do i z naprawy pokrywa Wykonawca, • Naprawy gwarancyjne urządzeń muszą być realizowane przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. <p>Do każdego zestawu komputerowego dołączony antywirus:</p> <p>Przeznaczony do kompleksowej ochrony serwerów i stacji klienckich pracujących pod kontrolą systemów z rodziny Microsoft Windows. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.</p> <p>Licencja w postaci subskrypcji czasowej min. 12 miesięcy</p> <p>Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer</p> <p>1. Oprogramowanie klienckie, zarządzane z poziomu serwera.</p> <p>System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance +.</p> <p>Silnik musi umożliwiać co najmniej:</p> <ul style="list-style-type: none"> • wykrywanie i blokowanie plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji, • wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych, • stosowanie kwarantanny, • wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear) • skanowanie urządzeń USB natychmiast po podłączeniu, • automatyczne odłączanie zainfekowanej końcówki od sieci, • skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób pełni konfigurowalny w stosunku do podejmowanych akcji w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji. • Zarządzanie „aktywami” stacji klienckiej, zbierające informacje co najmniej o nazwie komputera, producencie i modelu komputera, przynależności do grupy roboczej/domeny, szczegółach systemu operacyjnego, lokalnych kontach użytkowników, dacie i godzinie 	
--	--	---	--

		<p>uruchomienia i ostatniego restartu komputera, parametrach sprzętowych (proc., RAM, SN, storage), BIOS, interfejsach sieciowych, dołączonych peryferiach.</p> <ul style="list-style-type: none"> • Musi posiadać moduł ochrony IDS/IPS • Musi posiadać mechanizm wykrywania skanowania portów • Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów • Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości <p>Szyfrowanie danych:</p> <ul style="list-style-type: none"> • Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows. • Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom. • Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach. <p>Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:</p> <ul style="list-style-type: none"> • Przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli • Zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory • Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux • Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet. • Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością 	
--	--	---	--

		<p>eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich</p> <ul style="list-style-type: none"> Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji <p>Zarządzanie przez Chmurę:</p> <ul style="list-style-type: none"> Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej <p>System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:</p> <ul style="list-style-type: none"> różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD funkcje regulowania połączeń WiFi i Bluetooth funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi funkcje blokowania dostępu dowolnemu urządzeniu możliwość tymczasowego dodania dostępu do urządzenia przez administratora zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora 	
--	--	--	--

		<ul style="list-style-type: none"> • możliwość zarządzania urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry • możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich • funkcję wirtualnej klawiatury • możliwość blokowania każdej aplikacji • możliwość zablokowania aplikacji w oparciu o kategorie • możliwość dodania własnych aplikacji do listy zablokowanych • zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientów poprzez konsole administracyjną na serwerze • dodawanie innych aplikacji • dodawanie aplikacji w formie portable • możliwość wyboru pojedynczej aplikacji w konkretnej wersji • dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB • kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool • możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki. • możliwość zablokowania funkcji Printscreen • funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSX • funkcje monitorowania i kontroli przepływu poufnych informacji • możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukiwania w różnych typów plików • możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj • możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe • ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe • ochrona zawartości schowka systemu • ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL • możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych • ochrona plików zamkniętych w archiwach • Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem • możliwość tworzenia profilu DLP dla każdej polityki • wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania • ochrona przed wyciekiem plików poprzez programy typu p2p • Monitorowanie zmian w plikach: 	
--	--	---	--

		<ul style="list-style-type: none"> ○ Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych. ○ Funkcje monitorowania określonych rodzajów plików. ○ Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania. ○ Generator raportów do funkcjonalności monitora zmian w plikach. ○ możliwość śledzenia zmian we wszystkich plikach ○ możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach ○ możliwość definiowania własnych typów plików • Optymalizacja systemu operacyjnego stacji klienckich: <ul style="list-style-type: none"> ○ usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku ○ optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem ○ możliwość zaplanowania optymalizacji na wskazanych stacjach klienckich ○ instruktaż stanowiskowy pracowników Zamawiającego ○ dokumentacja techniczna w języku polskim <p>Wspierane platformy i systemy operacyjne:</p> <ul style="list-style-type: none"> • Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit) • Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit) • Mac OS X, Mac OS 10 • Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat, 	
2	Zestaw komputerowy (Typ B)	<p>Typ: Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta</p> <p>Zastosowanie: Komputer będzie wykorzystywany do kształcenia na kierunku technik organizacji reklamy potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, aplikacji sieciowych, aplikacji serwerowych, tworzenia grafik 2D i 3D oraz renderingu wideo, wirtualizacji systemów operacyjnych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna</p> <p>Wydajność obliczeniowa: Procesor klasy x86 ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach stacjonarnych, taktowany zegarem co najmniej 3,2 GHz, pamięcią last level cache CPU co najmniej 12 MB lub równoważny. Procesor powinien osiągać w teście wydajności PassMark PerformanceTest (wynik dostępny: http://www.passmark.com/products/pt.htm) co najmniej wynik minimum 15120 punktów Passmark CPU Mark – Załącznik Nr 8 do SIWZ</p> <p>Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testu Oferent musi udostępnić Zamawiającemu</p>	16

	<p>licencjonowane oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego.</p> <p>Pamięć operacyjna: 16 GB DDR4 2666 MHz możliwość rozbudowy do min 32 GB, minimum jeden slot wolny na dalszą rozbudowę pamięci</p> <p>Parametry pamięci masowej: Wewnętrzny dysk twardy SSD o pojemności min. 256 GB, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii bez dodatkowych nośników.</p> <p>Dodatkowo wewnętrzny dysk twardy o pojemności min. 1000 GB SATA, 7200 obr./min.</p> <p>Wydajność grafiki: Dedykowana wewnętrzna karta graficzna z własną pamięcią RAM o pojemności 2 GB, wyposażona w złącza min. 3 x mini DisplayPort, osiągająca min. 1450 pkt w teście Videocard Benchmark (http://www.videocardbenchmark.net/) – Załącznik 9 do SIWZ</p> <p>oraz zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki, ze wsparciem dla DirectX 12, OpenGL 4.5, osiągająca min. 1190 pkt w teście Videocard Benchmark (http://www.videocardbenchmark.net/) – Załącznik 9 do SIWZ</p> <p>Wyposażenie multimedialne: Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, porty słuchawek i mikrofonu na przednim oraz na tylnym panelu obudowy, obudowa wyposażona w głośnik.</p> <p>Obudowa i zasilacz</p> <p>Obudowa przystosowana do pracy w pionie.</p> <p>Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż pojedynczego dysku twardego 3,5 cala, napędu optycznego, kart rozszerzeń oraz obudowy.</p> <p>Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki).</p> <p>Obudowa musi być wyposażona w głośnik.</p> <p>Obudowa musi być wyposażona w zamek na klucz chroniący dostęp do wnętrza komputera – zamek nie może wystawiać poza obrys obudowy komputera.</p> <p>Obudowa musi być wyposażona w czujnik otwarcia obudowy współpracujący z oprogramowaniem diagnostyczno-monitorującym producenta komputera. Po aktywacji czujnika zdarzenie otwarcia obudowy musi być rejestrowane w logu dostępnym w ustawieniach BIOS komputera.</p> <p>Obudowa typu mini tower z obsługą kart PCI Express wyłącznie o pełnym profilu, wyposażona w min. 5 kieszeni: min. 2 szt. 5,25" zewnętrzne (dopuszcza się maksymalnie jedną zatokę na napęd optyczny typu SLIM), min. 1 szt. 3,5" wewnętrzne, min. 1 szt. 3,5" zewnętrzna.</p>	
--	--	--

		<p>W celu szybkiej weryfikacji usterki w obudowę komputera musi być wbudowany akustyczny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami. Obudowa musi być wyposażona w pokrywę chroniącą gniazda na tylnej ścianie komputera przed niepowołanym dostępem i przed przypadkowym wypięciem kabli zamykana za pomocą zamka blokującego dostęp do wnętrza komputera.</p> <p>Zasilacz o mocy minimum 280W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 94%, przy 50% obciążeniu - wymagane jest dostarczenie karty katalogowej produktu potwierdzające te parametry. Suma wymiarów obudowy (wysokość + szerokość + głębokość mierzona po krawędziach zewnętrznych) nie może wynosić więcej niż 860 mm.</p> <p>BIOS</p> <ul style="list-style-type: none"> – Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: <ul style="list-style-type: none"> ○ Modelu komputera ○ Numerze seryjnym ○ wersji BIOS, ○ dacie produkcji BIOS, ○ ilości, częstotliwości taktowania i sposobu obłożenia kanałów pamięciami RAM, ○ modelu płyty głównej ○ nazwie komputera ○ typie procesora wraz z informacją o częstotliwości taktowania ○ producencie, modelu oraz pojemności zainstalowanego dysku twardego ○ MAC adresie zintegrowanej karty sieciowej – Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS) – Możliwość z poziomu BIOS-u włączenia/wyłączenia funkcji automatycznej aktualizacji BIOS-u. System powinien umożliwiać zdefiniowanie adresu IP serwera TFTP w sieci lokalnej lub podanie nazwy serwera, w którego bezpośrednio z poziomu BIOS-u można dokonać aktualizacji BIOS-u. System powinien umożliwiać również określenie częstotliwości sprawdzania dostępności nowszej wersji BIOS-u z częstotliwością co najmniej: raz dziennie, raz na tydzień, raz na miesiąc i raz na kwartał. – Możliwości aktualizacji BIOS-u w tym co najmniej: całkowite wyłączenie możliwości aktualizacji, możliwość aktualizacji za pomocą narzędzi producenta komputera lub mechanizmu Windows Update, możliwość aktualizacji jedynie za pomocą narzędzi producenta komputera 	
--	--	---	--

		<ul style="list-style-type: none"> – Możliwość włączania/wyłączania sprzętowego wsparcia wirtualizacji w procesorze liczby aktywnych rdzeni procesora; – Możliwość włączania/wyłączania technologii SpeedStep oraz Turbo – Możliwość wyboru trybu pracy systemu chłodzenia komputera spośród co najmniej w trzech ustawień: automatyczny, maksymalna wydajność CPU oraz maksymalna prędkość wentylatorów. – Możliwość monitorowania temperatury rdzenia procesora, obudowy procesora oraz temperatury wewnątrz obudowy komputera oraz prędkości obrotowej wentylatora. – Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznymi urządzeniami – Możliwość ustawienia trybu pracy komputera po przywróceniu zasilania po awarii zasilania w co najmniej trzech trybach: pozostaje wyłączony, zawsze wyłączony, zawsze włączony, przywrócenie stanu z przed awarii – 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 (dla wszystkich rodzajów dysków twardych w tym dysków M.2). – Możliwość ustawienia poziomu zabezpieczenia BIOS-u za pomocą hasła co najmniej na dwóch poziomach: – Standardowy: umożliwiający skasowanie hasła za pomocą zworki na płycie głównej – Silny: umożliwiający zresetowanie hasła jedynie poprzez interwencję serwisu – Młączenia/wyłączenia zintegrowanej karty dźwiękowej, karty sieciowej, modułu TPM z poziomu BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. – Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. – Możliwość wyłączenia portów USB w tym: wszystkich portów, tylko portów znajdujących się na przedzie obudowy, tylko tylnych portów, tylko zewnętrznych, wszystkich nieużywanych. W przypadku włączenia jedynie przednich lub jedynie tylnych lub jedynie używanych portów wymagana jest możliwość określenia czy włączone mają być jedynie porty USB do których podłączona jest klawiatura i mysz lub możliwość wyłączenia portów do których podłączone są pamięci masowe lub hub USB. 	
--	--	--	--

		<p>Dodatkowe oprogramowanie</p> <p>Oprogramowanie dostarczone przez producenta komputera pozwalające na zdalną inwentaryzację komputerów w sieci, lokalną i zdalną inwentaryzację komponentów komputera, umożliwiające co najmniej:</p> <ul style="list-style-type: none"> – Informowanie administratora o otwarciu obudowy – Zdalne wyłączenie, restart oraz hibernacje komputera w sieci, – Otrzymywanie informacji WMI – Windows Management Interface, – Tworzenie raportów stanu jednostki, – Monitorowanie stanu komponentów: CPU, Pamięć RAM, HDD, wersje BIOS, – Aktualizację BIOS do najnowszej wersji zarówno dla pojedynczej maszyny jak i grupy, – Tworzenie kopii zapasowych BIOS wraz z ustawieniami – Tworzenie indywidualnych numerów dla poszczególnych użytkowników, – Włączenie lub wyłączenie BOOTowania portów USB – W pełni automatyczną instalację sterowników urządzeń opartą o automatyczną detekcję posiadanego sprzętu – Certyfikowane oprogramowanie umożliwiające w bezpieczny (bezpowrotny) sposób usunięcie danych z dysku twardego z poziomu BIOS-u bez względu na stań czy obecność systemu operacyjnego – w ofercie należy podać nazwę oprogramowania oraz producenta <p>Wymagania dodatkowe:</p> <ul style="list-style-type: none"> • Wbudowane porty minimalnie: <ul style="list-style-type: none"> – 1 x DVI-D – 1 x Display Port 1.2 – 1 x eSATA – 1 x RJ-45 – 1 x Czytnik kart pamięci z przodu obudowy – 1 x Audio: line-in – 1 x Audio: line-out – 1 x Audio: mikrofon z przodu obudowy – 1 x Audio: słuchawki z przodu obudowy – 8 szt. USB w tym: minimum 4 porty z przodu obudowy (w tym min. 2 x USB 3.0), minimum 4 porty z tyłu obudowy (w tym min. 2 x USB 3.0. Porty te powinny być wlutowane w płytę główną – nie dopuszcza się portów wyprowadzonych z płyty głównej na zewnątrz komputera za pomocą przewodów, taśm itp. <p>Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.</p>	
--	--	---	--

		<ul style="list-style-type: none"> Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika) 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 (TPM co najmniej w wersji 2.0) Płyta główna z wbudowanymi: <ul style="list-style-type: none"> 1 złącze PCI-Express 2.0 x4 (mech. x16) 1 złącze PCI-Express 3.0 x16 1 złącze M.2-2280 umożliwiające zamontowanie modułu SSD NVMe (PCI-Express 2.0) Minimum 2 złącza DIMM z obsługą do 32GB DDR4 pamięci RAM, min. 3 złącz SATA 3.0 NCQ, min. 1x złącze m.2 2280, płyta musi być trwale oznaczona logo producenta komputera Klawiatura w układzie QWERTY US Mysz przewodowa z trzema klawiszami oraz rolką (scroll) min. 1000 dpi Wewnętrzna nagrywarka DVD +/-RW <p>Normy i standardy</p> <p>Komputery mają spełniać normy i posiadać deklaracje zgodności (lub inne dokumenty potwierdzające spełnienie norm) w zakresie:</p> <ul style="list-style-type: none"> Deklaracja zgodności CE normy Energy Star 7.0 Certyfikat EPEAT na poziomie GOLD dla Polski - wymagany wpis dotyczący oferowanego modelu komputera w internetowym katalogu http://www.epeat.net - dopuszcza się wydruk ze strony internetowej Być wykonane/wyprodukowane w systemie zapewnienia jakości ISO 9001/14001 <p>Wymienione wyżej normy i deklaracje jakości mogą być zastąpione normami i deklaracjami jakości równoważnymi. Wykonawca będzie miał obowiązek wykazania, że wskazane normy i deklaracje równoważne zapewniają tę samą jakość i bezpieczeństwo dostarczonych komputerów, co normy i deklaracje wskazane przez Zamawiającego.</p> <p>Zamawiający wymaga:</p> <ul style="list-style-type: none"> dla potwierdzenia, że oferowany sprzęt odpowiada postawionym wymaganiom i był wykonany przez Wykonawcę (a jeżeli Wykonawca nie jest producentem to przez producenta) w systemie zapewnienia jakości wg normy ISO 9001 aby Wykonawca 	
--	--	---	--

		<p>posiadał: Certyfikat ISO 9001 lub inne zaświadczenie/dokument wydane przez niezależny podmiot zajmujący się poświadczaniem zgodności działań wykonawcy z normami jakościowymi odpowiadającej normie ISO 9001 (załączyć dokument potwierdzający spełnianie wymogu).</p> <ul style="list-style-type: none"> Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia wykonawcy wystawionego na podstawie dokumentacji producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram. Gwarancja jakości producenta: <ul style="list-style-type: none"> Na okres co najmniej 36 miesięcy - świadczonej w siedzibie Zamawiającego, chyba że niezbędne będzie naprawa sprzętu w siedzibie producenta lub autoryzowanym przez niego punkcie serwisowym - wówczas koszt transportu do i z naprawy pokrywa Wykonawca, Czas reakcji na zgłoszoną reklamację gwarancyjną - do końca następnego dnia roboczego Naprawy gwarancyjne urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta, Wsparcie techniczne producenta <ul style="list-style-type: none"> 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 – do oferty należy dołączyć link strony. <p>System operacyjny: Microsoft Windows 10 Professional PL lub równoważny.</p> <p>Opis równoważności:</p> <p>Nie wymagający aktywacji za pomocą Internetu lub telefonu.</p> <p>Zainstalowany system operacyjny, w polskiej wersji językowej.</p>	
--	--	---	--

	<p>Dołączony nośnik optyczny (CD/DVD) z instalatorem systemu operacyjnego oraz wszystkimi niezbędnymi do poprawnej pracy zestawu komputerowego sterownikami – parametry techniczne i funkcjonalne systemu.</p> <p>System operacyjny klasy desktop, 64-bit.</p> <p>Dostępne dwa rodzaje graficznego interfejsu użytkownika poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji, w tym:</p> <ol style="list-style-type: none"> 1) klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy; 2) dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych. <p>Interfejsy użytkownika dostępne w wielu językach do wyboru, w tym:</p> <ol style="list-style-type: none"> 1) polskim; 2) angielskim. <p>Zlokalizowane w języku polskim, co najmniej następujące elementy:</p> <ol style="list-style-type: none"> 1) menu; 2) odtwarzacz multimedialny; 3) pomoc; 4) komunikaty systemowe. <p>Wbudowany system pomocy w języku polskim.</p> <p>Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim.</p> <p>Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego.</p> <p>Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika.</p> <p>Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne.</p> <p>Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.</p> <p>Wbudowana zaporę internetową (firewall) dla ochrony połączeń internetowych.</p> <p>Zintegrowana z systemem operacyjnym konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.</p> <p>Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.</p> <p>Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi).</p> <p>Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer.</p> <p>Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji.</p>	
--	--	--

		<p>Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji.</p> <p>Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe.</p> <p>Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie.</p> <p>Możliwość pracy systemu w trybie ochrony kont użytkowników.</p> <p>Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu.</p> <p>Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów, w tym:</p> <ol style="list-style-type: none"> 1) poziom menu; 2) poziom otwartego okna systemu operacyjnego. <p>Wbudowany system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych.</p> <p>Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.</p> <p>Obsługa standardu NFC (near field communication).</p> <p>Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).</p> <p>Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.</p> <p>Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.</p> <p>Mechanizmy logowania do domeny w oparciu o:</p> <ol style="list-style-type: none"> 1) login i hasło; 2) karty z certyfikatami (smartcard); 3) wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM). <p>Mechanizmy wieloelementowego uwierzytelniania.</p> <p>Wsparcie dla uwierzytelniania na bazie Kerberos v. 5.</p> <p>Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu.</p> <p>Wsparcie dla algorytmów Suite B (RFC 4869).</p> <p>Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec.</p> <p>Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk.</p> <p>Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.</p> <p>Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń.</p>	
--	--	--	--

	<p>Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.</p> <p>Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową.</p> <p>Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację.</p> <p>Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający niezawodność i pozwalający tworzyć kopie zapasowe.</p> <p>Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.</p> <p>Udostępnianie modemu.</p> <p>Wbudowane oprogramowanie do tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.</p> <p>Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.</p> <p>Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).</p> <p>Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).</p> <p>Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych.</p> <p>Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika.</p> <p>Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w układzie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB.</p> <p>Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych.</p> <p>Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.</p> <p>Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.</p> <p>Do każdego zestawu komputerowego dostarczony monitor:</p>	
--	--	--

		<p>Typ ekranu: Panoramiczny; ciekłokrystaliczny z aktywną matrycą IPS 24" (nie mniej niż 23,8 cala), utwardzany (3H);</p> <p>Jasność: min. 250 cd/m²</p> <p>Możliwość obrotu (Swivel): min. 340°;</p> <p>Pilot: tak</p> <p>Kontrast: min. 1000:1</p> <p>Wielkość plamki (maks): 0,2745 mm</p> <p>Kąty widzenia (pion/poziom): min. 178°/178° (CR10:1)</p> <p>Czas reakcji matrycy: max 5 ms</p> <p>Możliwość zmiany wysokości (min.): 15 cm</p> <p>Kolory: min. 16,7 mln</p> <p>Rozdzielczość maksymalna: 1920 x 1080 pikseli</p> <p>Powłoka powierzchni ekranu: Przeciwodblaskowa, utwardzona (3H)</p> <p>Zakres pochylenia monitora (min.): Od -5° do +35°</p> <p>Złącze (min): 15-stykowe złącze D-Sub, DVI-D (z HDCP), HDMI</p> <p>Średnie użycie energii (maks.): 15 W</p> <p>Inne: Monitor musi posiadać usuwalną podstawę montażową, wbudowane min. 2 głośniki min. 2W, oraz hub USB min. 2x USB 2.0; kompatybilność z VESA 100 mm, Kensington Lock</p> <p>Dołączone oprogramowanie producenta monitora pozwalające na zdalne sprawdzenie parametrów pracy oraz konfigurację ustawień monitora</p> <p>Normy i standardy:</p> <p>Monitory muszą być wykonane zgodnie normami i posiadać certyfikaty: TCO 7.0, ISO9241-307, EPEAT Gold, Energy Star 7.0, TÜV Low Blue Light, TÜV Flicker Free – lub inne dokumenty wdane przez niezależny podmiot uprawniony do kontroli jakości, potwierdzające, że dostarczone monitory odpowiadają wskazanym normom.</p> <p>Wymienione wyżej normy i deklaracje jakości mogą być zastąpione normami i deklaracjami jakości równoważnymi. Wykonawca będzie miał obowiązek wykazania, że wskazane normy i deklaracje równoważne zapewniają tę samą jakość i bezpieczeństwo dostarczonych komputerów, co normy i deklaracje wskazane przez Zamawiającego.</p> <p>Gwarancji jakości producenta:</p> <ul style="list-style-type: none"> – Na okres co najmniej 36 miesięcy - świadczonej w siedzibie Zamawiającego, chyba że niezbędne będzie naprawa sprzętu w siedzibie producenta lub autoryzowanym przez niego punkcie serwisowym - wówczas koszt transportu do i z naprawy pokrywa Wykonawca, – Naprawy gwarancyjne urządzeń muszą być realizowane przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. <p>Do każdego zestawu komputerowego dołączony antywirus:</p>	
--	--	--	--

		<p>Przeznaczony do kompleksowej ochrony serwerów i stacji klienckich pracujących pod kontrolą systemów z rodziny Microsoft Windows.</p> <p>Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.</p> <p>Licencja w postaci subskrypcji czasowej min. 12 miesięcy</p> <p>Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer</p> <ul style="list-style-type: none"> – Oprogramowanie klienckie, zarządzane z poziomu serwera. <p>System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance +.</p> <p>Silnik musi umożliwiać co najmniej:</p> <ul style="list-style-type: none"> – wykrywanie i blokowanie plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji, – wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych, – stosowanie kwarantanny, – wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear) – skanowanie urządzeń USB natychmiast po podłączeniu, – automatyczne odłączanie zainfekowanej końcówki od sieci, – skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w stosunku do podejmowanych akcji w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji. – Zarządzanie „aktywami” stacji klienckiej, zbierające informacje co najmniej o nazwie komputera, producencie i modelu komputera, przynależności do grupy roboczej/domeny, szczegółach systemu operacyjnego, lokalnych kontach użytkowników, dacie i godzinie uruchomienia i ostatniego restartu komputera, parametrach sprzętowych (proc., RAM, SN, storage), BIOS, interfejsach sieciowych, dołączonych peryferiach. – Musi posiadać moduł ochrony IDS/IPS – Musi posiadać mechanizm wykrywania skanowania portów – Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów – Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości <p>Szyfrowanie danych:</p>	
--	--	---	--

		<ul style="list-style-type: none"> – Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows. – Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom. – Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach. <p>Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:</p> <ul style="list-style-type: none"> – Przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli – Zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory – Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux – Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet. – Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich – Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji <p>Zarządzanie przez Chmurę:</p> <ul style="list-style-type: none"> – Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach 	
--	--	---	--

		<ul style="list-style-type: none"> – Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury – Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur – Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy – Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach – Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urzędów – Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej <p>System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:</p> <ul style="list-style-type: none"> – różne ustawienia dostępu dla urzędów: pełny dostęp, tylko do odczytu i blokowanie – funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD – funkcje regulowania połączeń WiFi i Bluetooth – funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe – funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi – funkcje blokowania dostępu dowolnemu urządzeniu – możliwość tymczasowego dodania dostępu do urządzenia przez administratora – zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu – możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka – możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora – możliwość zarządzania urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry – możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich – funkcję wirtualnej klawiatury – możliwość blokowania każdej aplikacji – możliwość zablokowania aplikacji w oparciu o kategorie – możliwość dodania własnych aplikacji do listy zablokowanych – zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientów poprzez konsolę administracyjną na serwerze 	
--	--	---	--

		<ul style="list-style-type: none"> – dodawanie innych aplikacji – dodawanie aplikacji w formie portable – możliwość wyboru pojedynczej aplikacji w konkretnej wersji – dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB – kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool – możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki. – możliwość zablokowania funkcji Printscreen – funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx – funkcje monitorowania i kontroli przepływu poufnych informacji – możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików – możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj – możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe – ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe – ochrona zawartości schowka systemu – ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL – możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych – ochrona plików zamkniętych w archiwach – Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem – możliwość tworzenia profilu DLP dla każdej polityki – wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania – ochrona przed wyciekiem plików poprzez programy typu p2p – Monitorowanie zmian w plikach: <ul style="list-style-type: none"> ○ Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych. ○ Funkcje monitorowania określonych rodzajów plików. ○ Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania. ○ Generator raportów do funkcjonalności monitora zmian w plikach. ○ możliwość śledzenia zmian we wszystkich plikach ○ możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach 	
--	--	---	--

		<ul style="list-style-type: none"> ○ możliwość definiowania własnych typów plików – Optymalizacja systemu operacyjnego stacji klienckich: <ul style="list-style-type: none"> ○ usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku ○ optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem ○ możliwość zaplanowania optymalizacji na wskazanych stacjach klienckich ○ instruktaż stanowiskowy pracowników Zamawiającego ○ dokumentacja techniczna w języku polskim <p>Wspierane platformy i systemy operacyjne:</p> <ul style="list-style-type: none"> – Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit) – Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit) – Mac OS X, Mac OS 10 – Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat 	
3	Komputer przenośny	<p>Typ: Komputer przenośny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta</p> <p>Zastosowanie: Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna</p> <p>Wydajność obliczeniowa: Procesor klasy x86 ze zintegrowaną grafiką, czterordzeniowy, ośmiowątkowy zaprojektowany do pracy w komputerach przenośnych, taktowany zegarem co najmniej 2,3 GHz, pamięcią last level cache CPU co najmniej 8 MB lub równoważny. Procesor powinien osiągać w teście wydajności PassMark PerformanceTest (wynik dostępny: http://www.passmark.com/products/pt.htm) co najmniej wynik minimum 9430 punktów Passmark CPU Mark – Załącznik Nr 8 do SIWZ</p> <p>Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testu Oferent musi udostępnić Zamawiającemu licencjonowane oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego.</p> <p>Pamięć operacyjna: min.16 GB DDR4 2400 MHz możliwość rozbudowy do min. 32 GB,</p> <p>Parametry pamięci masowej: Wewnętrzny dysk twardy SSD o pojemności min. 240 GB, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii bez dodatkowych nośników.</p> <p>Wydajność grafiki: zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki, ze wsparciem</p>	16

	<p>dla DirectX 12, OpenGL 4.5, osiągająca min. 1190 pkt w teście Videocard Benchmark (http://www.videocardbenchmark.net/) – Załącznik Nr 9 do SIWZ</p> <p>Dedykowana karta graficzna posiadająca pamięć wbudowaną na min. 4 GB pamięci GDDR5, ze wsparciem dla DirectX 12, OpenGL 4.5, osiągająca min. 4650 pkt w teście Videocard Benchmark (http://www.videocardbenchmark.net/) – Załącznik Nr 9 do SIWZ</p> <p>Wyposażenie multimedialne: Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, porty słuchawek i mikrofonu (dopuszczalny port Combo), 2 wbudowane głośniki, wbudowany mikrofon, wbudowana kamera min. 1 Mpix</p> <p>Matryca (min.): 15,6", podświetlana LED, IPS, o rozdzielczości natywnej 1920x1080 pikseli, matowa</p> <p>Złącza:</p> <ul style="list-style-type: none"> • 1x 10/100/1000 Mbps LAN RJ-45 • USB 3.1 Gen. 1 – min. 2 szt. • USB 2.0 – min. 1 szt. • HDMI – min. 1 szt. • Czytnik kart pamięci – min. 1 szt. • Wejście mikrofon/słuchawki – min. 1 szt. • Gniazdo zasilania – 1 szt. <p>Łączność: Bluetooth, WiFi 802.11 a/b/g/n/ac, LAN 10/100/1000 Mbps</p> <p>Waga (maks.): 2,3 kg</p> <p>Bateria (min.): 5250 mAh</p> <p>Dodatkowe wymagania: możliwość zabezpieczenia linką, wydzielona klawiatura numeryczna</p> <p>System operacyjny: Microsoft Windows 10 Professional PL lub równoważny.</p> <p>Opis równoważności:</p> <p>Nie wymagający aktywacji za pomocą Internetu lub telefonu.</p> <p>Zainstalowany system operacyjny, w polskiej wersji językowej.</p> <p>Dołączony nośnik optyczny (CD/DVD) z instalatorem systemu operacyjnego oraz wszystkimi niezbędnymi do poprawnej pracy zestawu komputerowego sterownikami – parametry techniczne i funkcjonalne systemu.</p> <p>System operacyjny klasy desktop, 64-bit.</p> <p>Dostępne dwa rodzaje graficznego interfejsu użytkownika poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji, w tym:</p> <ol style="list-style-type: none"> 1) klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy; 2) dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych. <p>Interfejsy użytkownika dostępne w wielu językach do wyboru, w tym:</p> <ol style="list-style-type: none"> 1) polskim; 	
--	--	--

	<p>2) angielskim. Zlokalizowane w języku polskim, co najmniej następujące elementy:</p> <ol style="list-style-type: none"> 1) menu; 2) odtwarzacz multimedialny; 3) pomoc; 4) komunikaty systemowe. <p>Wbudowany system pomocy w języku polskim. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modulem „uczenia się” pisma użytkownika – obsługa języka polskiego. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modulem „uczenia się” głosu użytkownika. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. Wbudowana zaporę internetową (firewall) dla ochrony połączeń internetowych. Zintegrowana z systemem operacyjnym konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 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. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie. Możliwość pracy systemu w trybie ochrony kont użytkowników. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów, w tym:</p> <ol style="list-style-type: none"> 1) poziom menu; 	
--	---	--

	<p>2) poziom otwartego okna systemu operacyjnego.</p> <p>Wbudowany system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych.</p> <p>Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.</p> <p>Obsługa standardu NFC (near field communication).</p> <p>Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).</p> <p>Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.</p> <p>Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.</p> <p>Mechanizmy logowania do domeny w oparciu o:</p> <ol style="list-style-type: none"> 1) login i hasło; 2) karty z certyfikatami (smartcard); 3) wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM). <p>Mechanizmy wieloelementowego uwierzytelniania.</p> <p>Wsparcie dla uwierzytelniania na bazie Kerberos v. 5.</p> <p>Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu.</p> <p>Wsparcie dla algorytmów Suite B (RFC 4869).</p> <p>Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec.</p> <p>Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk.</p> <p>Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.</p> <p>Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń.</p> <p>Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązywania problemu z komputerem.</p> <p>Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową.</p> <p>Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację.</p> <p>Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający niezawodność i pozwalający tworzyć kopie zapasowe.</p> <p>Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.</p> <p>Udostępnianie modemu.</p>	
--	---	--

		<p>Wbudowane oprogramowanie do tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.</p> <p>Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.</p> <p>Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).</p> <p>Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).</p> <p>Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych.</p> <p>Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika.</p> <p>Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w układzie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB.</p> <p>Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych.</p> <p>Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.</p> <p>Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.</p> <p>Do każdego komputera przenośnego dołączony antywirus:</p> <p>Przeznaczony do kompleksowej ochrony serwerów i stacji klienckich pracujących pod kontrolą systemów z rodziny Microsoft Windows.</p> <p>Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.</p> <p>Licencja w postaci subskrypcji czasowej min. 12 miesięcy</p> <p>Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer</p> <p>Oprogramowanie klienckie, zarządzane z poziomu serwera.</p> <p>System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance +.</p> <p>Silnik musi umożliwiać co najmniej:</p> <ul style="list-style-type: none"> wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji, 	
--	--	---	--

		<ul style="list-style-type: none"> wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych, stosowanie kwarantanny, wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear) skanowanie urządzeń USB natychmiast po podłączeniu, automatyczne odłączanie zainfekowanej końcówki od sieci, skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w stosunku do podejmowanych akcji w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji. Zarządzanie „aktywami” stacji klienckiej, zbierające informacje co najmniej o nazwie komputera, producencie i modelu komputera, przynależności do grupy roboczej/domeny, szczegółach systemu operacyjnego, lokalnych kontach użytkowników, dacie i godzinie uruchomienia i ostatniego restartu komputera, parametrach sprzętowych (proc., RAM, SN, storage), BIOS, interfejsach sieciowych, dołączonych peryferiach. Musi posiadać moduł ochrony IDS/IPS Musi posiadać mechanizm wykrywania skanowania portów Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości <p>Szyfrowanie danych:</p> <ul style="list-style-type: none"> Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows. Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom. Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach. 	
--	--	--	--

		<p>Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:</p> <ul style="list-style-type: none"> • Przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli • Zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory • Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux • Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet. • Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich • Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji <p>Zarządzanie przez Chmurę:</p> <ul style="list-style-type: none"> • Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach • Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury • Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur • Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy • Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach • Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń • Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej 	
--	--	--	--

		<p>System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:</p> <ul style="list-style-type: none"> • różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie • funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD • funkcje regulowania połączeń WiFi i Bluetooth • funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe • funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi • funkcje blokowania dostępu dowolnemu urządzeniu • możliwość tymczasowego dodania dostępu do urządzenia przez administratora • zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu • możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka • możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora • możliwość zarządzania urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry • możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich • funkcję wirtualnej klawiatury • możliwość blokowania każdej aplikacji • możliwość zablokowania aplikacji w oparciu o kategorie • możliwość dodania własnych aplikacji do listy zablokowanych • zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsolę administracyjną na serwerze • dodawanie innych aplikacji • dodawanie aplikacji w formie portable • możliwość wyboru pojedynczej aplikacji w konkretnej wersji • dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB • kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool • możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki. • możliwość zablokowania funkcji Printscreen • funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx • funkcje monitorowania i kontroli przepływu poufnych informacji 	
--	--	---	--

		<ul style="list-style-type: none"> • możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukiwania w różnych typów plików • możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj • możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe • ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe • ochrona zawartości schowka systemu • ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL • możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych • ochrona plików zamkniętych w archiwach • Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem • możliwość tworzenia profilu DLP dla każdej polityki • wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania • ochrona przed wyciekiem plików poprzez programy typu p2p • Monitorowanie zmian w plikach: <ul style="list-style-type: none"> ○ Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych. ○ Funkcje monitorowania określonych rodzajów plików. ○ Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania. ○ Generator raportów do funkcjonalności monitora zmian w plikach. ○ możliwość śledzenia zmian we wszystkich plikach ○ możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach ○ możliwość definiowania własnych typów plików • Optymalizacja systemu operacyjnego stacji klienckich: <ul style="list-style-type: none"> ○ usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku ○ optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem ○ możliwość zaplanowania optymalizacji na wskazanych stacjach klienckich ○ instruktaż stanowiskowy pracowników Zamawiającego ○ dokumentacja techniczna w języku polskim <p>Wspierane platformy i systemy operacyjne:</p>	
--	--	---	--

		<ul style="list-style-type: none"> • Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit) • Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit) • Mac OS X, Mac OS 10 • Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat 	
4	Oprogramowanie biurowe	<p>Microsoft Office 2019 Pro lub równoważny - pakiet aplikacji biurowych musi zawierać:</p> <ul style="list-style-type: none"> • Edytor tekstów • Arkusz kalkulacyjny • Narzędzie do przygotowywania i prowadzenia prezentacji • Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) • Bazy danych <p>Edytor tekstów musi umożliwiać:</p> <ul style="list-style-type: none"> • 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, • Wstawianie oraz formatowanie tabel, Wstawianie oraz formatowanie obiektów graficznych, • Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne), • Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków, • Automatyczne tworzenie spisów treści, • Formatowanie nagłówków i stopek stron, • Sprawdzanie pisowni w języku polskim, • Śledzenie zmian wprowadzonych przez użytkowników, • Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, • Określenie układu strony (pionowa/pozioma), • Wydruk dokumentów, • Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną, • Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2000, XP, 2003, 2007, 2010, 2013 i 2016 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu, • Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji, 	48

		<ul style="list-style-type: none"> • 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, • Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa, • Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze i pozwalające zapisać plik wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i Prawnych. <p>Arkusz kalkulacyjny musi umożliwiać:</p> <ul style="list-style-type: none"> • Tworzenie raportów tabelarycznych, • Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych, • Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu, • Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice), • Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych, • Wyszukiwanie i zamianę danych, • Wykonywanie analiz danych przy użyciu formatowania warunkowego, • Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie, • Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, • Formatowanie czasu, daty i wartości finansowych z polskim formatem, • Zapis wielu arkuszy kalkulacyjnych w jednym pliku, • Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2000, XP, 2003, 2007, 	
--	--	--	--

		<p>2010, 2013 i 2016 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń,</p> <ul style="list-style-type: none"> • Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. <p>Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:</p> <ul style="list-style-type: none"> • Przygotowywanie prezentacji multimedialnych, które będą prezentowane przy użyciu projektora multimedialnego, • Drukowanie w formacie umożliwiającym robienie notatek, • Zapisanie jako prezentacja tylko do odczytu, • Nagrywanie narracji i dołączanie jej do prezentacji, • Opatrywanie slajdów notatkami dla prezentera, • Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo, • Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego, • Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym, • Możliwość tworzenia animacji obiektów i całych slajdów, • Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, • Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2000, XP, 2003, 2007, 2010, 2013 i 2016. <p>Narzędzie do zarządzania informacją prywatną (poczta elektroniczna, kalendarzem, kontaktami i zadaniami) musi umożliwiać:</p> <ul style="list-style-type: none"> • Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, • Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców, • Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, • Automatyczne grupowanie poczty o tym samym tytule, • Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy, • Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, • Zarządzanie kalendarzem, • Udostępnianie kalendarza innym użytkownikom, 	
--	--	---	--

		<ul style="list-style-type: none"> • Przeglądanie kalendarza innych użytkowników, • Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach, • Zarządzanie listą zadań, • Zlecanie zadań innym użytkownikom, • Zarządzanie listą kontaktów, • Udostępnianie listy kontaktów innym użytkownikom, • Przeglądanie listy kontaktów innych użytkowników, • Możliwość przesyłania kontaktów innym użytkownikom. <p>Narzędzie do tworzenia i pracy z lokalną bazą danych musi umożliwiać:</p> <ul style="list-style-type: none"> • tworzenie bazy danych przez zdefiniowanie: <ul style="list-style-type: none"> a) tabel składających się z unikatowego klucza i pól różnych typów, w tym tekstowych i liczbowych, b) relacji pomiędzy tabelami, formularzy do wprowadzania i edycji danych, c) raportów, • edycję danych i zapisywanie ich w lokalnie przechowywanej bazie danych, • tworzenie bazy danych przy użyciu zdefiniowanych szablonów, połączenie z danymi zewnętrznymi, a w szczególności z innymi bazami danych zgodnymi z ODBC, plikami XML, arkuszem kalkulacyjnym, <p>Licencja dożywotnia, przeznaczona dla podmiotów edukacyjnych, dostarczona w formie licencji zbiorczej.</p>	
5	Oprogramowanie graficzne (Typ A)	<p>Oprogramowanie graficzne CorelDRAW 2019 lub oprogramowanie równoważne.</p> <p>Za oprogramowanie równoważne Zamawiający uzna inne produkty posiadające zachowany zakres funkcjonalności powyższych programów.</p> <p>W tym minimum:</p> <p>Zawartość pakietu:</p> <p>Program do tworzenie grafiki wektorowej i układu stron</p> <p>Program do edycji zdjęć</p> <p>Program do przeglądania czcionek i zarządzanie nimi</p> <p>Program do przekształcania map bitowych do postaci wektorowej</p> <p>Program do wyszukiwania zasobów</p> <p>Program do przechwytywania zawartości ekranu</p> <p>Program do edycji zdjęć w formacie RAW</p> <p>Program do projektowania graficznego online w przeglądarce internetowej.</p> <p>Moduł dodatkowy służący do powiększania obrazów cyfrowych</p> <p>Zasoby</p>	2

		<p>Minimum 7 000 obrazków clipart i obrazków cyfrowych oraz szablonów grafik na pojazdy Minimum 1000 zdjęć o wysokiej rozdzielczości Minimum 1000 czcionek TrueType i OpenType Minimum 150 zaprojektowanych szablonów Minimum 600 rodzajów wypełnień mapą bitową, wektorowych i tonalnych</p> <p>Dokumentacja i szkolenia Przewodnik szybkiego startu Karta szybkiego wyszukiwania Pliki Pomocy ONLINE Szkoleniowe nagrania wideo online Okres licencjonowania: wieczysty Ilość licencji: Licencja zbiorcza na 16 stanowisk</p>	
6	Oprogramowanie graficzne (Typ B)	<p>Oprogramowanie graficzne Corel Videostudio PRO 2019 lub oprogramowanie równoważne. Za oprogramowanie równoważne Zamawiający uzna inne produkty posiadające zachowany zakres funkcjonalności powyższych programów. W tym minimum: Wymagania systemowe: Windows 10, Windows 8, Windows 7, 64-bitowy Wymagania procesora: Intel Core i3 lub AMD A4 3.0 GHz lub wyższy Intel Core i5 lub i7 1.06 GHz lub wyższy wymagany dla wsparcia AVCHD & Intel Quick Sync Video Intel Core i7 lub AMD Athlon A10 lub wyższy dla UHD, Multi-Camera lub 360° video Wymagania pamięci: 4 GB RAM lub więcej, 8 GB rekomendowane dla UHD, Multi-Camera, lub 360° video Wymagania grafiki: 256 MB VRAM Wymagania ekranu: Minimalna rozdzielczość: 1024 x 768 Wymagania dysku: minimum 4 GB wolnego miejsca</p> <p>Obsługiwane formaty importu Video: AVI, DivX*, DV, DVR-MS, HDV, HEVC (H.265), M2T, M2TS, M4V, MKV, MOD, MOV (H.264), MPEG-1/-2/-4, SWF*, TOD, UIS, UISX, WebM, WMV, XAVC S, 3GP, Non-encrypted DVD titles Audio: AAC, Aiff, AMR, AU, CDA, M4A, MOV, MP3, MP4, MPA, OGG, WAV, WMA Image: CLP, CUR, DCS, DCX, EPS, FAX, FPX, GIF87a, ICO, IFF, IMG, JP2, JPC, JPG, MAC, MPO, MSP, PBM, PCT, PCX, PGM, PIC, PNG<, PPM, PSD, PSPIImage, PXR, RAS, SCI, SCT, SHG, TGA, TIF/TIFF, UFO, UFP, WBM, WBMP, WMF, 001, Camera RAW</p> <p>Obsługiwane formaty Exportu: Video: AVI, DV, HDV, HEVC (H.265), M2T, MOV, MPEG-1/-2/-4, UIS, UISX, WebM, WMV, 3GP</p>	2

		<p>Device: Apple iPod/iPhone/iPad/TV, Sony PSP/PS3/PS4, Nintendo Wii, Microsoft Xbox compatible formats</p> <p>Audio: AC3, M4A, OGG, WAV, WMA</p> <p>Image: BMP, JPG</p> <p>Wsparcie dla technologii Blu-ray</p> <p>Okres licencjonowania: wieczysty</p> <p>Ilość licencji: Licencja zbiorcza na 16 stanowisk</p>	
7	Oprogramowanie graficzne (Typ C)	<p>Oprogramowanie graficzne Corel PaintShop PRO 2019 lub oprogramowanie równoważne.</p> <p>Za oprogramowanie równoważne Zamawiający uzna inne produkty posiadające zachowany zakres funkcjonalności powyższych programów.</p> <p>W tym minimum:</p> <p>Obsługiwane systemy operacyjne: Windows 10, Windows 8 / 8.1, Windows 7 z najnowszym service pack (64-bitowe lub 32-bitowe)</p> <p>Wymagania procesora: Intel Core Duo 1,8 GHz, Core i3 lub AMD Athlon 64 X2 3800+ 2,0 GHz lub szybszy</p> <p>Wymagania pamięci: 2 GB pamięci RAM lub więcej (minimum 4 GB dla Windows 64bit)</p> <p>Wymagania karty graficznej: 128 MB VRAM VGA</p> <p>Wymagania dysku twardego: 1 GB wolnego miejsca na dysku twardym wymagane (zalecane 2 GB)</p> <p>Wymagania dot. monitora: 1280 x 768 z 16-bitowym kolorowym wyświetlaczem (rozdzielczość 768 x 1366 z 24-bit lub wyższa kolorowy wyświetlacz zalecane)</p> <p>Obsługiwane formaty importu: AI, BMP, CAL, CALS, CGM, CLP, CUR, CUT, DCX, DIB, EMF, EPS, GIF, HDP, IFF, IMG, J2C, J2K, JIF, JP2, JPC, JPE, JPEG, JPG, JPS, JPX, MAC, MPO, MRW, MSP, PBM, PCD *, PCT, PCX, PDF, PGM, PIC, PICT, PNG, PNS, PPM, PS, PSD, PSP (pliki graficzne PSP), RAS, RAW, RIF, RLE, SCT, SVG, SVGZ, TGA, TIF, UFO, WBM, WBMP, WDP, WebP, WMF, WPG</p> <p>Obsługiwane formaty Brush: PaintShop Pro Brush (.pspbrush), Adobe Photoshop Brush (.abr) Jasc Brush (.jbr)</p> <p>Obsługiwane formaty eksportu: BMP, CAL, CALS, CLP, CUT, DCX, DIB, EMF, EPS, AI, PS, GIF, HDP, WDP, IFF, IMG, JP2, J2C, J2K, JPC, JPX, JPG, JIF, JPE, JPEG, MAC, MSP, PBM, PCX, PGM, PIC, PPM, PNG, PSD, PSP (PSPIMAGE FILES), RAS, RAW, RIF, RIFF, RLE, SCT, JPS, PNS, TGA, TIF, TIFF, WBMP, WBM, WebP, WMF</p> <p>Okres licencjonowania: wieczysty</p> <p>Ilość licencji: Licencja zbiorcza na 16 stanowisk</p>	2
8	Drukarka laserowa kolorowa	<p>Typ drukarki: laserowa</p> <p>Druk w kolorze: Tak</p> <p>Szybkość druku w A4 (minimum): 30 str./min. w kolorze, 30 str/min. w mono</p> <p>Czas wydruku pierwszej strony (maksymalnie): 8 sekund</p> <p>Szybkość procesora: 510 MHz</p>	8

		<p>Rozdzielczość druku (minimum): 1200x1200 dpi</p> <p>Pamięć RAM (minimum): 1024 MB</p> <p>Czcionki druku (minimum): 87 skalowanych czcionek PCL, 80 czcionek PostScript</p> <p>Język druku (minimum): PCL5c, PCL6, SIDM, PostScript 3 emulacja, XPS</p> <p>Dupleks: Tak, mechaniczny</p> <p>Złącza (minimum): Port USB 2.0, Ethernet 10/100/1000 BaseTX</p> <p>Podajnik papieru 1: 250 arkuszy 80 g/m², formaty papieru A4, A5, B5, A6.</p> <p>Podajnik papieru 2: 100 arkuszy 80 g/m²</p> <p>Obsługiwane formaty papieru (min.): A4, A5, B5, A6, Monarch, Com-9, Com-10, DL, CS, nośnik (baner) do 130 cm długości</p> <p>Gramatura papieru (min.): 64-220 g/m²</p> <p>Odbiornik papieru (min.): 150 stron</p> <p>Obciążenie miesięczne (min.): 58000 stron</p> <p>Zużycie energii w trybie bezczynności (maks.): 90W</p> <p>Dokumenty: Oświadczenie producenta sprzętu, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.</p> <p>Certyfikat ISO 9001:2008 producenta oferowanego sprzętu - dokumenty potwierdzające załączyć do oferty.</p> <p>Certyfikat ISO 14001:2004 producenta oferowanego sprzętu - dokumenty potwierdzające załączyć do oferty.</p>	
9	Tonery do drukarki laserowej	<p>Komplet tonerów do drukarki z poz. 8</p> <p>Przez komplet Zamawiający rozumie (minimum):</p> <p>1x toner black</p> <p>1x toner cyan</p> <p>1x toner magenta</p> <p>1x toner yellow</p> <p>Tonery dedykowane do drukarki, oryginalne lub rekomendowane przez producenta urządzenia z punktu 9</p> <p>Zamawiający wymaga, by zastosowane tonery nie spowodowały utraty gwarancji na dostarczone drukarki (opisane w poz. 8)</p>	8
10	Ploter	<p>Typ urządzenia: Ploter</p> <p>Rodzaj druku: termiczny</p> <p>Druk w kolorze: Tak</p> <p>Obsługiwane formaty papieru (min.): A4, A3, A2, A1, A0</p> <p>Rozdzielczość druku (min.): 2400x1200 dpi</p> <p>Prędkość druku w czerni (min.): 0,5 str./min. (format A1)</p> <p>Obsługiwana gramatura papieru: 60-270 g/m²</p> <p>Zainstalowana pamięć (min.): 1024 MB</p> <p>Porty (min.): 1x USB 2.0, 1x RJ-45</p> <p>Łączność Wi-Fi: Tak</p>	6
11	Tusze do plotera	<p>Komplet tuszy do plotera z poz. 10</p> <p>Przez komplet Zamawiający rozumie (minimum):</p> <p>2x tusz black</p>	24

		1x tusz cyan 1x tusz magenta 1x tusz yellow Tusze dedykowane do plotera, oryginalne lub rekomendowane przez producenta urządzenia z punktu 11. Zamawiający wymaga, by zastosowane tusze nie spowodowały utraty gwarancji na dostarczone plotery (opisane w poz. 10)	
12	Skaner	Typ urządzenia: Skaner płaski Typ sensora: optyczny CIS Rozdzielczość natywna (min.): 4800 x 4800 dpi Rozmiar skanowania (min.): A4 Prędkość skanowania (min.): 10 s/stronę Porty (min.): 1x USB Pobór mocy (maksymalnie): 2,5W	8
13	Telewizor	Przekątna ekranu (minimum): 75" Rozdzielczość (minimum): 3840x2160 pikseli Typ matrycy: LED Odświeżanie (minimum): 50 Hz Procesor: czterordzeniowy HDR: Tak Złącza (minimum): 1x RJ-45, 2x USB, wyjście optyczne, 1x kompozytowe, 4x HDMI, 1x złącze CI Łączność bezprzewodowa (minimum): Bluetooth, WiFi 802.11 ac Głośniki (minimum): 40W Rodzaj głośników: 2,1 CH Odtwarzanie USB Roczne zużycie energii (maksymalnie): 277 W	3
14	Słuchawki multimedialne	Typ: nauszne Impedancja (minimum): 31 Ohm Poziom głośności (minimum): 109 dB Pasma przenoszenie słuchawek (minimum): 40 -18000 Hz Wbudowany mikrofon: Tak Pismo przenoszenia mikrofonu (minimum): 80 – 15000 Hz Kierunkowa charakterystyka mikrofonu Długość przewodu (minimum): 3m Złącza (minimum): 1x USB	32
15	Zestaw głośników	Typ zestawu: 2.1 Moc niskotowa RMS (minimum): 15,5W Moc głośnika satelitarnego RMS (minimum): 5W Zakres częstotliwości (minimum): 40-20000 Hz Ekranowanie magnetyczne: Tak Pilot do sterowania: Tak Typ podłączenia: jack 3,5mm	2
16	Projektor	Rozdzielczość (min.): FullHD 1920x1080 Technologia wyświetlania: DLP Proporcje obrazu: 16:9	2

		<p>Jasność (min.): 3500 ANSI Lumenów</p> <p>Współczynnik kontrastu (min.): 19000:1</p> <p>Głośność w trybie normalnym (max.): 27 dB</p> <p>Żywotność lampy: tryb normalny (min.) 3500 godz. /tryb ECO 10000 godz.</p> <p>Porty (min.): 1x HDMI, 1x VGA (wejście), 1x złącze kompozytowe, 2x Audio 3,5mm, 1x USB-A</p> <p>Port sterowania (min.): 9-pin D-Sub przez RS-232</p> <p>Głośnik (min.): 10W</p>	
--	--	--	--