Załącznik nr 1

Szczegółowy Opis Przedmiotu Zamówienia

Część I – Zakup i dostawa sprzętu komputerowego dla Szkoły Podstawowej nr 1 im. Juliana Tuwima w Pajęcznie.

1. Komputer AiO 23,8" –

……

Podać producenta, model i dokładny pn urządzenia

l.p.	NAZWA KOMPONENTU	WYMAGANE PARAMETRY TECHNICZNE
1	**Typ obudowy**	• zintegrowana z monitorem typu All In One, nie dopuszcza się, aby jakiekolwiek kable przyłączeniowe pomiędzy ekranem a innymi elementami komputera były widoczne i wystawały poza obudowę • wbudowane głośniki stereo • wbudowana kamera 5,0 Mpix
2	**Monitor**	• min. 23,8", Full HD 1920x1080, Jasność matrycy 250 nit
3	**Procesor**	• dwurdzeniowy, czterowątkowy; taktowanie: min 2,5 GHz (bez Turbo), min. 3,5 GHz dla trybu Turbo; osiągający wynik min. 4150 na stronie porównywarki PassMark® Software Pty Ltd (na dzień nie wcześniejszy niż 15.03.2021)
4	**Pamięć RAM**	• min. 8 GB DDR4 SO-DIMM
5	**Dysk twardy**	• min. 256 GB m.2 PCI-Express 2280
6	**Karta graficzna**	• Zintegrowana, osiągająca wynik min. 1,100 na stronie porównywarki PassMark® Software Pty Ltd (na dzień nie wcześniejszy niż 15.03.2021)
7	**Płyta główna**	Posiada porty: • Min. 1 x HDMI • min. 4 x USB typu A (w tym min. 2 x USB 3.0 typu A) • audio
8	**Łączność**	• wbudowane Wi-Fi 802.11a/b/g/n/ac • wbudowane min. 1 x RJ45 Gigabit LAN • wbudowany Bluetooth

9	**System operacyjny**	• Windows 10 Pro 64 bit (nie dopuszcza się wersji edukacyjnej)
10	**Klawiatura i mysz**	• Klawiatura USB qwerty w kolorze obudowy komputera • mysz optyczna USB w kolorze obudowy komputera
11	**Gwarancja**	• producenta min. 36 miesięcy On-site (realizowana w miejscu eksploatacji) - nie dopuszcza się gwarancji dystrybutora, Wykonawcy • możliwość sprawdzenia na stronie producenta po podaniu numeru seryjnego rodzaju oraz okresu gwarancji
12	**Inne**	• Komputer pochodzi z Polskiej dystrybucji oraz został wyprodukowany nie wcześniej niż w 2020r. • Zamawiający wymaga, aby producent oferowanych urządzeń posiadał certyfikat ISO 9001 – **załączyć do oferty** • Zamawiający wymaga, aby producent oferowanych urządzeń posiadał certyfikat ISO 14001 - **załączyć do oferty** • Zamawiający wymaga, aby urządzenie posiadało certyfikat CE lub deklarację zgodności CE - **załączyć do oferty** • Zamawiający wymaga, aby serwis urządzeń był realizowany przez producenta lub autoryzowanego partnera serwisowego producenta oraz zgodnie z wymaganiami normy ISO 9001 - **załączyć do oferty ISO dla serwisu** • Zamawiający wymaga, aby zapewniony był dostęp do najnowszych sterowników i uaktualnień na stronie internetowej producenta realizowany poprzez podanie modelu urządzenia lub numeru seryjnego

2. Projektor krótkoogniskowy -

……

Podać producenta, model i dokładny pn urządzenia

1	**Technologia wyświetlania**	• DLP
2	**Rozdzielczość podstawowa**	• 1080p Full HD (1920x1080)
3	**Jasność**	• Min. 2 900 lumenów
4	**Kontrast**	• Min. 18 000:1
5	**Korekcja trapezowa**	• +/-40°
6	**Lampa**	• Moc min. 188W

		• Żywotność min. 4500h w trybie Normalnym oraz 5500h w trycie Eco
7	**Odległość wyświetlania**	• Co najmniej w zakresie 0,58m – 3,30m
8	**Wejścia / wyjścia**	• Min. 2 x HDMI (w tym min. 1 x z MHL) • Min. 1 x audio 3,5” • Min. 1 x USB
9	**Głośnik**	• Min. 8W
10	**Zasilanie**	• Zasilanie 230V • Zużycie energii w trybie czuwania maks. 1W • Zużycie energii w trybie pracy – maks. 245W
11	**Inne**	• Język OSD – polski • Blokada Kensington • Obsługa 3D • Podświetlany pilot • Projektor ma współpracować z zaproponowaną tablicą interaktywną
12	**Gwarancja**	• Min. 36 miesięcy gwarancji producenta - nie dopuszcza się gwarancji dystrybutora, Wykonawcy • Zamawiający wymaga przeglądu projektora, czyszczenia z kurzu po roku oraz po 2 latach eksploatacji – wykonane na miejscu w miejscu eksploatacji
13	**Montaż**	• Wymagany przez Zamawiającego montaż, konfiguracja, kalibracja oraz szkolenie. Szkolenie odbędzie się w wyznaczonym przez dyrektora terminie • Montaż projektora na uchwycie ściennym nad tablicą, maksymalna odległość projektora od ściany 1,20m • Dostarczenie uchwytu ściennego umożliwiającego montaż ścienny w odległości 1,20m od ściany, wymaganego okablowania (HDMI 10m, przewody zasilające) wszelkie akcesoria montażowe po stronie Wykonawcy

3. Tablica interaktywna -

.....

Podać producenta, model i dokładny pn urządzenia

1	**Powierzchnia**	• stalowa, lakierowana magnetyczna
2	**Rozmiar**	• przekątna min. 94” • przekątna obszaru interaktywnego min. 89”
3	**Śledzenie sygnału**	• 6 ms - 12 ms
4	**Precyzja**	• ± 0.5 mm

5	**Dotyk**	• Sterowanie za pomocą pisaka, palca bądź innych nieprzezroczystych obiektów • 10 – TOUCH - jednoczesna praca dziesięciu osób bez konieczności dzielenia obszaru roboczego na 10 stref
6	**Technologia**	• Podczerwień
7	**Inne**	• suchościeralna o wysokiej odporności na zarysowania i uszkodzenia mechaniczne • matowa antyodblaskowa powierzchnia • technologia rozpoznawania gestów multi-gesture • dostosowana do używania pisaków suchościeralnych; • rozpoznawanie pisma odręcznego • odtwarzanie video z możliwością „pisania" na filmie • zrzuty video • szybkie tworzenie figur geometrycznych • biblioteka załączników związanych z przedmiotami szkolnymi • integracja z programami MS Office pozwalająca na ręczne dopisywanie notatek do dokumentów
8	**Głośniki**	• wymagane w zestawie dedykowane przez producenta tablicy głośniki o mocy min. 38W • sterowane za pomocą kabla USB • Hub posiadający przyciski + i – do regulacji głośności • możliwość regulacji głośności suwakiem w systemie operacyjnym
9	**Certyfiakty**	• Zamawiający wymaga, aby producent oferowanych urządzeń posiadał certyfikat ISO 9001 – załączyć do oferty • Zamawiający wymaga, aby producent oferowanych urządzeń posiadał certyfikat ISO 14001 - załączyć do oferty • Zamawiający wymaga, aby urządzenie posiadało certyfikat CE lub deklarację zgodności CE - załączyć do oferty
10	**Gwarancja**	• Min. 36 miesięcy gwarancji
11	**Montaż**	• W ramach dostawy Zamawiający wymaga montażu, konfiguracji, kalibracji oraz szkolenia. Szkolenie odbędzie się w wyznaczonym przez dyrektora terminie. Wszystkie dodatkowe elementy montażowe po stronie Wykonawcy.

Część II – Zakup i dostawa sprzętu komputerowego dla Szkoły Podstawowej im. Jana Brzechwy w Makowiskach.

Komputer prznośny -

……

Podać producenta, model i dokładny pn urządzenia

Komputer przenośny	**8 sztuki**
Procesor	Osiągający w testach CPU Benchmark PassMark min. 5150 punktów na dzień 26.02.2021r. Procesor musi się znajdować na liście PassMark stanowiącej załącznik nr 7 do SIWZ. Taktowanie podstawowe 1.2 GHz (w trybie turbo 3,6 GHz) Pamięć podręczna 4MB Maksymalne TDP 15W
Matryca	Rozmiar 15,6” Rozdzielczość natywna 1920x1080 Powierzchnia matowa Typ matrycy: MVA+ Jasność: min. 220 nit
Dysk	256GB PCIe m.2 NVMe Gen. 3 x4
Pamięć RAM	8GB DDR4 z taktowaniem 3200 MHz z możliwością rozbudowy do 32GB DDR4 1 gniazdo pamięci wolne
Karta graficzna	Osiągający w testach Video Card Benchmark PassMark min. 1850 punktów na dzień 26.02.2021r. Karta graficzna musi się znajdować na liście PassMark stanowiącej załącznik nr 8 do SIWZ.
Klawiatura	QWERTY PL Wydzielona klawiatura numeryczna
Sterowanie	Touchpad
Porty	2x USB 3.0 typ A 1x USB 3.0 typ C 1x USB 2.0 typ A 1x HDMI 1x RJ-45 1x gniazdo słuchawek / mikrofonu (combo) Zamawiający nie dopuszcza stosowania przejściówek, adapterów, stacji dokujących i innych rozwiązań dodatkowych w celu osiągnięcia wymaganych portów

Łączność	Zintegrowany port LAN: 10/100/100 Mbps Zintegrowana (wbudowana w komputer) karta sieci bezprzewodowej WiFi: 802.11 a/b/g/n/ac Zintegrowana (wbudowana w komputer) karta sieci Bluetooth
Multimedia	2 wbudowane głośniki stereo Wbudowana kamera o rozdzielczości 0,9 Mpix Wbudowany mikrofon Wbudowany czytnik kart pamięci microSD / SD
Bateria i zasilanie	3 komorowy Min. 32Wh
Budowa i waga	Obudowa w kolorze szarym lub czarnym Maksymalna grubość 20mm Maksymalna głębokość 250mm Maksymalna szerokość 365mm Maksymalna waga 2,0 kg
Bezpieczeństwo	Zintegrowany z procesorem lub wbudowany w płytę główną moduł TPM 2.0
Gwarancja	24 miesiące w standardzie Door-to-Door Serwis producenta komputera lub autoryzowanego partnera producenta komputera. Zamawiający nie dopuszcza gwarancji Wykonawcy, lub podmiotów zewnętrznych nie posiadających autoryzacji Producenta komputera. Koszt odbioru i zwrotu z serwisu pokrywa Producent lub Wykonawca
System operacyjny	Microsoft Windows 10 Professional PL w wersji komercyjnej lub edukacyjnej. System zainstalowany przez producenta komputera. Zamawiający dopuszcza rozwiązanie równoważne: System zainstalowany przez producenta komputera. Nie wymagający aktywacji za pomocą Internetu lub telefonu. Zainstalowany system operacyjny, w polskiej wersji językowej. Dołączony nośnik optyczny (CD/DVD) z instalatorem systemu operacyjnego oraz wszystkimi niezbędnymi do poprawnej pracy zestawu komputerowego sterownikami – parametry techniczne i funkcjonalne systemu. System operacyjny klasy desktop, 64-bit. Dostępne dwa rodzaje graficznego interfejsu użytkownika poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji, w tym: 1) klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy; 2) dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych. Interfejsy użytkownika dostępne w wielu językach do wyboru, w tym: 1) polskim; 2) angielskim. Zlokalizowane w języku polskim, co najmniej następujące elementy: 1) menu; 2) odtwarzacz multimediów; 3) pomoc; 4) komunikaty systemowe. Wbudowany system pomocy w języku polskim. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia

	się” pisma użytkownika – obsługa języka polskiego. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „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 zapora internetowa (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: 1) poziom menu; 2) poziom otwartego okna systemu operacyjnego. Wbudowany system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych.

	Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. Obsługa standardu NFC (near field communication). Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. Mechanizmy logowania do domeny w oparciu o: 1) login i hasło; 2) karty z certyfikatami (smartcard); 3) wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM). Mechanizmy wieloelementowego uwierzytelniania. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu. Wsparcie dla algorytmów Suite B (RFC 4869). Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową. Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający niezawodność i pozwalający tworzyć kopie zapasowe. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. Udostępnianie modemu. Wbudowane oprogramowanie do tworzenia kopii zapasowych (Backup); automatyczne

	wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 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.). Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika. 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. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinsatalacji systemu.
Oprogramowanie antywirusowe	
Rodzaj i funkcje	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.
Czas licencji	12 miesięcy
Architektura	Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer Oprogramowanie klienckie, zarządzane z poziomu serwera.
Podstawowa funkcjonalność	System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance +. Silnik musi umożliwiać co najmniej:

	• wykrywanie i blokowania 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 Szyfrowanie danych: • 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
Zarządzanie i administracja	Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej: • 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 Zarządzanie przez Chmurę: 1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach 2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury 3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur 4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy 5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach 6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń 7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej
Kontrola urządzeń, aplikacji i DLP	System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej: • 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 zarządzani 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 konsole administracyjna 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 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 przez wyciekiem plików poprzez programy typu p2p
Dodatkowe wymagania	Monitorowanie zmian w plikach: • 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 definiowana własnych typów plików Optymalizacja systemu operacyjnego stacji klienckich: • usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku

	• optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem • możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich • instruktaż stanowiskowy pracowników Zamawiającego • dokumentacja techniczna w języku polskim Wspierane platformy i systemy operacyjne: • 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.