

**Załącznik nr 1 „Opis przedmiotu umowy
wymagane parametry”**

1. Laptopy – 24 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne	Spełnia / nie spełnia
Zastosowanie	Komputer przenośny będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna.	
Ekran	Matryca TFT, min. 15,6” z podświetleniem w technologii LED, powłoka antyrefleksyjna Anti-Glare- rozdzielczość: FHD 1920x1080, 220nits	
Obudowa	Obudowa komputera matowa, zawiasy metalowe. Kąt otwarcia matrycy min.130 stopni. W obudowę wbudowane co najmniej 2 diody sygnalizujące stan naładowania akumulatora oraz pracę dysku twardego.	
Wydajność obliczeniowa	Procesor klasy x86, osiągający wynik co najmniej 3200 pkt w teście PassMark CPU Mark, według wyników opublikowanych na stronie http://www.cpubenchmark.net lub http://www.passmark.com Dostarczyć wydruk z jednej z powyższych stron internetowych na wezwanie zamawiającego	
Płyta główna	Wyposażona w interfejs SATA III (6 Gb/s) do obsługi dysków twardych	
Pamięć operacyjna RAM	8GB, możliwość rozbudowy do 16 GB	
Pamięć masowa	256GB SSD M.2 zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.	
Wydajność grafiki	Karta graficzna musi osiągać wynik co najmniej 800 pkt. w teście PassMark 3D Graphics Mark, według wyników opublikowanych na stronie http://www.videocardbenchmark.net lub http://www.passmark.com Dostarczyć wydruk z jednej z powyższych stron internetowych na wezwanie zamawiającego	
Klawiatura	Klawiatura wyspowa, układ US z wydzielonym blokiem numerycznym.	
Audio/Video	Wbudowana karta dźwiękowa, zgodna z HD Audio; Wbudowane głośniki stereo 2 x 1,5W; Wbudowany mikrofon; Sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze; Wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute); Kamera HD720p;	

Karta sieciowa	10/100/1000 – RJ 45	
Porty/złącza	2 x USB 3.1, 1 x USB 2.0,, złącze słuchawek i złącze mikrofonu typu COMBO, 1 x HDMI, RJ-45, czytnik kart multimedialnych (min SD/SDHC/SDXC).	
WiFi	Wbudowana karta sieciowa, pracująca w standardzie AC	
Bluetooth	Wbudowany moduł Bluetooth 4.2	
Bateria	Bateria – 3-komorowa, 30 WHr pozwalająca na nieprzerwaną pracę urządzenia do 6 godzin.	
Zasilacz	Zasilacz zewnętrzny o mocy maksymalnej 45W	
Waga	Maksymalnie 2 kg;	
BIOS	<p>BIOS zgodny ze specyfikacją UEFI.</p> <p>Możliwość odczytania z BIOS bez uruchamiania systemu operacyjnego, informacji o:</p> <ul style="list-style-type: none"> - wersji BIOS - nr seryjnym komputera - ilości pamięci RAM - typie procesora i jego prędkości -modelach zainstalowanych dysków twardych <p>Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności:</p> <ul style="list-style-type: none"> - możliwość ustawienia hasła dla twardego dysku - możliwość ustawienia hasła na starcie komputera tzw. POWER-On Password - możliwość ustawienia hasła Administratora i użytkownika BIOS - możliwość włączania/wyłączania wirtualizacji z poziomu BIOSU - możliwość wyłączania/włączania: zintegrowanej karty WIFI, portów USB, trybu PXE dla karty sieciowej, - 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. 	
Certyfikaty	Certyfikat ISO9001 lub certyfikat równoważny (dostarczyć na wezwanie Zamawiającego).	
Bezpieczeństwo	<ul style="list-style-type: none"> - złącze Kensington Lock, - TPM 2.0; 	
Oprogramowanie biurowe	<p>Zainstalowane oprogramowanie biurowe - kompletny pakiet oprogramowania biurowego musi spełniać następujące wymagania, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:</p> <p>1. Wymagania odnośnie interfejsu użytkownika:</p> <ul style="list-style-type: none"> a) Pełna polska wersja językowa interfejsu użytkownika; b) Prostota i intuicyjność obsługi, pozwalająca na prace osobom nieposiadającym umiejętności technicznych; c) Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active 	

	<p>Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej musi być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitorowania go o ponowne uwierzytelnienie się;</p> <p>2. Oprogramowanie musi umożliwiać tworzenie i edycje dokumentów elektronicznych w formacie, który spełnia następujące warunki:</p> <ul style="list-style-type: none"> a) posiada kompletny i publicznie dostępny opis formatu, b) ma zdefiniowany układ informacji w postaci XML zgodnie z Tabelą B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766) c) umożliwia wykorzystanie schematów XML d) wspiera w swojej specyfikacji podpis elektroniczny zgodnie z Tabelą A.1.1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766) <p>3. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb użytkownika oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców;</p> <p>4. Zamawiający wymaga licencji przeznaczonych wyłącznie dla jednostek edukacyjnych;</p> <p>5. W skład oprogramowania muszą wchodzić narzędzia umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami;</p> <p>6. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim;</p> <p>7. Pakiet zintegrowanych aplikacji biurowych musi zawierać:</p> <ul style="list-style-type: none"> a) Edytor tekstów b) Arkusz kalkulacyjny c) Narzędzie do przygotowywania i prowadzenia prezentacji d) Narzędzie do zarządzania informacją prywatną (poczta elektroniczna, kalendarzem, kontaktami i zadaniami) <p>8. Edytor tekstu musi umożliwiać:</p> <ul style="list-style-type: none"> a) Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności 	
--	---	--

	<p>gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty</p> <p>b) Wstawianie oraz formatowanie tabel</p> <p>c) Wstawianie oraz formatowanie obiektów graficznych</p> <p>d) Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne)</p> <p>e) Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków</p> <p>f) Automatyczne tworzenie spisów treści</p> <p>g) Formatowanie nagłówków i stopek stron</p> <p>h) Sprawdzanie pisowni w języku polskim</p> <p>i) Śledzenie zmian wprowadzonych przez użytkowników</p> <p>j) Nagrywanie, tworzenie i edycje makr automatyzujących wykonywanie czynności</p> <p>k) Określenie układu strony (pionowa/pozioma)</p> <p>l) Wydruk dokumentów</p> <p>m) Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną</p> <p>n) Prace na posiadanych przez zamawiającego dokumentach utworzonych przy pomocy Microsoft Word 2010, 2013 i 2016 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu</p> <p>o) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji</p> <p>p) 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.</p> <p>q) 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.</p> <p>r) Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze i</p>	
--	---	--

	<p>pozwalające zapisać plik wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i Prawnych.</p> <p>9. Arkusz kalkulacyjny musi umożliwiać:</p> <ul style="list-style-type: none"> a) Tworzenie raportów tabelarycznych b) Tworzenie wykresów liniowych (wraz linia trendu), słupkowych, kołowych c) Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu. d) Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice) e) Obsługę kostek OLAP oraz tworzenie i edycje kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych f) Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych g) Wyszukiwanie i zamianę danych h) Wykonywanie analiz danych przy użyciu formatowania warunkowego i) Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie j) Nagrywanie, tworzenie i edycje makr automatyzujących wykonywanie czynności k) Formatowanie czasu, daty i wartości finansowych z polskim formatem l) Zapis wielu arkuszy kalkulacyjnych w jednym pliku. m) Zachowanie pełnej zgodności z formatami posiadanych przez zamawiającego plików utworzonych za pomocą oprogramowania Microsoft Excel 2010, 2013 i 2016 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.. n) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji <p>10. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać przygotowywanie prezentacji multimedialnych oraz:</p> <ul style="list-style-type: none"> a) Prezentowanie przy użyciu projektora multimedialnego 	
--	--	--

	<ul style="list-style-type: none"> b) Drukowanie w formacie umożliwiającym robienie notatek c) Zapisanie w postaci tylko do odczytu. d) Nagrywanie narracji dołączanej do prezentacji e) Opatrywanie slajdów notatkami dla prezentera f) Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo g) Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego h) Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym i) Tworzenie animacji obiektów i całych slajdów j) Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera k) Pełna zgodność z formatami plików posiadanych przez zamawiającego, utworzonych za pomocą oprogramowania MS PowerPoint 2010, 2013 i 2016;. 	
	<p>11. Narzędzie do zarządzania informacją prywatną (poczta elektroniczna, kalendarzem, kontaktami i zadaniami) musi umożliwiać:</p> <ul style="list-style-type: none"> a) Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego b) Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców c) Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną d) Automatyczne grupowanie poczty o tym samym tytule e) Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy f) Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia g) Zarządzanie kalendarzem h) Udostępnianie kalendarza innym użytkownikom i) Przeglądanie kalendarza innych użytkowników j) Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach k) Zarządzanie listą zadań 	

	<ul style="list-style-type: none"> l) Zlecanie zadań innym użytkownikom m) Zarządzanie listą kontaktów n) Udostępnianie listy kontaktów innym użytkownikom o) Przeglądanie listy kontaktów innych użytkowników p) Możliwość przesyłania kontaktów innym użytkownikom 	
<p>Oprogramowanie zabezpieczające</p> <p>licencja aktualna przez okres co najmniej 24 miesięcy</p> <p>24 licencje</p>	<p>System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance+ musi umożliwiać co najmniej:</p> <ol style="list-style-type: none"> 1. Wykrywanie i blokowanie plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych, które używają czasie rzeczywistym algorytmów kompresji, 2. Wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych, 3. Stosowanie kwarantanny, 4. Wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear) 5. Skanowanie urządzeń USB natychmiast po podłączeniu, 6. Automatyczne odłączanie zainfekowanej końcówki od sieci, 7. 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. 8. Zarządzanie „aktywami” stacji klienckiej, zbierające informacje co najmniej o nazwie komputera, producencie i modelu komputera, przynależności do grupy roboczej/domeny, szczegółach systemu operacyjnego, lokalnych kontaktach użytkowników, dacie i godzinie uruchomienia i ostatniego restartu komputera, parametrach sprzętowych (proc. RAM, SN, dysk), BIOS, interfejsach sieciowych, dołączonych peryferiach. 9. Musi posiadać moduł ochrony IDS/IP 10. Musi posiadać mechanizm wykrywania skanowania portów 11. Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów 12. Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości 13. Oprogramowanie szyfrujące, chroniące dane za pomocą silnych algorytmów szyfrowania takich 	

	<p>jak AES, RC6, SERPENT i DWAFISH.</p> <ol style="list-style-type: none"> 14. Szyfrowanie całej zawartości na urządzeniach przenośnych, takich jak pendrive, dyski USB i udostępnianie ich tylko autoryzowanym użytkownikom. 15. Blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do komputera; 16. Definiowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do komputera; 17. Możliwość blokady zapisywania plików na zewnętrznych dyskach USB; 18. Blokada uruchamiania oprogramowania z takich dysków. 19. Blokada ta musi umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach. 20. Interfejs programu musi wyświetlać monity o zbliżającym się zakończeniu licencji, a także powiadamiać o zakończeniu licencji. 21. Moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware poprzez ograniczenie możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom. 22. Możliwość dowolnego zdefiniowania chronionych folderów; 23. Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów muszą mieć możliwość modyfikowania plików objętych ochroną any ransomware. 24. Monitorowanie krytycznych danych użytkownika zapobiegające atakom ransomware 25. Konsola zarządzająca umożliwiająca co najmniej: <ol style="list-style-type: none"> a) przechowywanie danych w bazie typu SQL; b) zdalną instalację lub deinstalację oprogramowania zabezpieczającego na komputerach, zakresie adresów IP lub grupie z ActiveDirectory; c) tworzenie paczek instalacyjnych oprogramowania, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux; d) centralną dystrybucję uaktualnień definicji ochronnych, z plików lub serwera konsoli, bez konieczności posiadania dostępu do internetu; e) raportowanie przez konsolę, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do 	
--	--	--

	<p>formatów CSV i PD</p> <p>f) definiowanie struktury opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji</p> <p>26. Wyświetlanie statusu bezpieczeństwa komputerów zlokalizowanych w różnych lokalizacjach;</p> <p>27. Tworzenie kopii zapasowych i przywracanie plików konfiguracyjnych z serwera;</p> <p>28. Możliwość tworzenia wielu poziomów dostępu, aby umożliwić dostęp do serwera zgodnie z przypisaniem do grupy</p> <p>29. Dostęp do konsoli zarządzającej z dowolnego miejsca;</p> <p>30. Możliwość przeglądania raportów sumarycznych dla wszystkich urządzeń;</p> <p>31. Wysyłanie raportów i powiadomień za pomocą poczty elektronicznej</p> <p>32. Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych i dystrybucji szyfrowania polityk bezpieczeństwa;</p> <p>33. Centralne zarządzanie informacjami odzyskiwania zaszyfrowanych danych;</p> <p>34. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z witryny producenta oprogramowania.</p> <p>35. Oprogramowanie, zarządzane z poziomu serwera.</p> <p>36. System musi umożliwiać co najmniej:</p> <ul style="list-style-type: none"> a) różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie b) przyznanie praw dostępu dla nośników pamięci tj. USB, CD c) regulowanie połączeń WiFi i Bluetooth d) kontrolowanie i regulowanie użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe e) blokowanie lub zezwalanie na połączenie z urządzeniami mobilnymi f) blokowanie dostępu dowolnemu urządzeniu; g) możliwość tymczasowego dodania dostępu do urządzenia; h) szyfrowanie zawartości USB i udostępnianie jej na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu; i) zablokowanie funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka; j) zezwalanie na dostęp tylko urządzeniom wcześniej dodanym przez administratora k) używania tylko zaufanych urządzeń sieciowych; 	
--	--	--

	<ul style="list-style-type: none"> l) funkcję wirtualnej klawiatury m) blokowanie każdej aplikacji n) zablokowanie aplikacji w oparciu o kategorie o) dodanie własnych aplikacji do listy zablokowanych p) tworzenie kompletnej listy aplikacji zainstalowanych na komputerach; q) wybór pojedynczej aplikacji w konkretnej wersji <p>37. Wymagane kategorie aplikacji: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool</p> <p>38. Możliwość generowania i wysyłania raportów o aktywności poprzez wymienne urządzenia i udziały sieciowe;</p> <p>39. Możliwość zablokowania funkcji Printscreen</p> <p>40. Monitorowanie przesyłu danych między aplikacjami;</p> <p>41. Blokowanie plików w oparciu o ich rozszerzenie lub rodzaj</p> <p>42. Monitorowanie i zarządzanie danymi udostępnianymi poprzez zasoby sieciowe</p> <p>43. Ochrona przed wyciekami informacji na drukarki lokalne i sieciowe, w poczcie e-mail i w komunikacji SSL;</p> <p>44. Ochrona zawartości schowka system</p> <p>45. Dodawanie wyjątków dla domen, aplikacji i lokalizacji sieciowych</p> <p>46. Ochrona plików zamkniętych w archiwach</p> <p>47. Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekami</p> <p>48. Możliwość tworzenia profilu dla każdej polityki</p> <p>49. Wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania</p> <p>50. Ochrona przed wyciekami plików poprzez programy typu p2p</p> <p>51. Monitorowanie działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.</p> <p>52. Monitorowanie określonych rodzajów plików.</p> <p>53. Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.</p> <p>54. Generator raportów na temat zmian w plikach.</p> <p>55. Możliwość śledzenia zmian we wszystkich plikach</p> <p>56. Możliwość śledzenia zmian w zainstalowanym oprogramowaniu</p> <p>57. Możliwość definiowania własnych typów plików do monitorowania</p> <p>58. Usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz</p>	
--	--	--

	<p>defragmentacji dysku;</p> <p>59. Optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem</p> <p>60. Możliwość zaplanowania optymalizacji na wskazanych komputerach;</p> <p>61. Dokumentacja techniczna w języku polskim</p> <p>62. Optymalizacja musi być realizowana za pomocą platformy w chmurze bez infrastruktury wewnątrz sieci firmowej.</p> <p>63. Zarządzanie użytkownikami przypisanymi do adresów email</p> <p>64. Przypisanie atrybutów do użytkowników, w tym co najmniej: Imię, Nazwisko, adres email, numer telefonu stacjonarnego, numer telefonu komórkowego, typ użytkownika</p> <p>65. Możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi</p> <p>66. Możliwość eksportu danych użytkownika</p> <p>67. Wdrożenie przez Email, SMS, kod QR;</p> <p>68. Import listy urządzeń z pliku CSV</p> <p>69. Podgląd co najmniej następujących informacji konfiguracji: data wdrożenia, status wdrożenia, status urządzenia, numer telefonu, właściciel, grupa, reguły, konfiguracja geolokacji, wersja oprogramowania zarządzającego;</p> <p>70. Podgląd co najmniej następujących informacji sprzętowych: model, producent, system, adres MAC, bluetooth, sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, zużycie procesora, moc sygnału;</p> <p>71. Podgląd lokacji urządzenia w zakresach czasu, tj. co najmniej: dzisiaj, wczoraj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres;</p> <p>72. Podgląd aktualnie zainstalowanych aplikacji</p> <p>73. Moduł raportowania aktywności, skanowania oraz naruszenia reguł musi umożliwiać podgląd co najmniej w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres</p> <p>74. Oprogramowanie do wykrywania oraz zarządzania podatnościami bezpieczeństwa umożliwiające</p> <ul style="list-style-type: none"> a) dostęp przez przeglądarkę internetową; b) portal zarządzający w postaci usługi hostowanej; <p>75. Portal zarządzający musi umożliwiać:</p> <ul style="list-style-type: none"> a) przegląd wybranych danych poprzez konfigurowalne widgety; b) zablokowanie możliwości zmiany konfiguracji widжетów; c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie 	
--	--	--

	<p>raportów; d) eksport skanów podatności do pliku CSV</p>	
System operacyjny	<p>System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:</p> <ol style="list-style-type: none"> 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: <ol style="list-style-type: none"> a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w języku polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitemi i przełączanie się pomiędzy pulpitemi za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z poziomów: menu, otwartego okna systemu operacyjnego; 7. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 8. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 9. Graficzne środowisko instalacji i konfiguracji w języku polskim 10. Wbudowany system pomocy w języku polskim. 11. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 12. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora Zamawiającego. 13. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 14. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, w tym możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 15. Zabezpieczony hasłem hierarchiczny dostęp do systemu; 16. Konta i profile użytkowników zarządzane zdalnie; 17. Praca systemu w trybie ochrony kont 	

	<p>użytkowników.</p> <p>18. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze;</p> <p>19. Możliwość zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".</p> <p>20. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na serwerze plików z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika</p> <p>21. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.</p> <p>22. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.</p> <p>23. Oprogramowanie dla tworzenia kopii zapasowych (Backup);</p> <p>24. Automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.</p> <p>25. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.</p> <p>26. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.</p> <p>27. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu);</p> <p>28. Wbudowany mechanizm wirtualizacji typu hypervisor;</p> <p>29. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem interfejsu graficznego.</p> <p>30. Bezpłatne biuletyny bezpieczeństwa związane z działaniem systemu operacyjnego.</p> <p>31. Wbudowana zaporę internetową (firewall) dla ochrony połączeń internetowych;</p> <p>32. Zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.</p> <p>33. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny;</p> <p>34. Zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej i udostępnianiem plików;</p>	
--	--	--

	<p>35. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików.</p> <p>36. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi i niez zarządzanymi.</p> <p>37. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne;</p> <p>38. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM</p> <p>39. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych;</p> <p>40. Możliwość tworzenia wirtualnych kart inteligentnych.</p> <p>41. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)</p> <p>42. Wsparcie dla IPSEC oparte na politykach;</p> <p>43. Wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;</p> <p>44. Mechanizmy logowania w oparciu o:</p> <ul style="list-style-type: none"> a) Login i hasło, b) Karty inteligentne i certyfikaty (smartcard), c) Wirtualne karty inteligentne i certyfikaty chronione poprzez moduł TPM; <p>45. Umożliwiający pracę w domenie;</p>	
Warunki gwarancji	<p>36 miesięcy gwarancji.</p> <p>Czas reakcji serwisu - do końca następnego dnia roboczego.</p>	

Oświadczam, że oferowane przez nas laptopy spełniają wszystkie powyższe wymagania.

.....
podpis Oferenta