**Opis przedmiotu zamówienia**

Przedmiotem zamówienia jest dostawa 177 sztuk fabrycznie nowych laptopów z oprogramowaniem w ramach programu „Wsparcie dzieci z rodzin pegeerowskich w rozwoju cyfrowym - Granty PPGR”. Wykonawca dostarczy przedmiot umowy zamawiającemu na koszt własny i dokona jego rozładunku i wniesienia do siedziby zamawiającego tj. Urząd Miasta Jarosławia, Rynek 1, 37-500 Jarosław.

|  |  |
| --- | --- |
| Atrybut  | Wymagania |
| Laptop | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna.Dostarczany sprzęt musi być fabrycznie nowy nie starszy niż wyprodukowany w 2021 roku. |
| Ekran | 15.6 FHD IPS (1920 x 1080), powłoką przeciwodblaskową, jasność 220 nits. Kąt otwarcia matrycy min.180 stopni |
| Obudowa | Obudowa komputera matowa, zawiasy metalowe. Kąt otwarcia matrycy min.180 stopni. W obudowie wbudowane co najmniej 2 diody sygnalizujące stan naładowania akumulatora oraz pracę dysku twardego. |
| Chipset | Dostosowany do zaoferowanego procesora |
| Płyta główna | Zaprojektowana i wyprodukowana przez producenta komputera wyposażona w interfejs PCIe oraz SATA III (6 Gb/s) do obsługi dysków twardych. |
| Wydajność komputera | Oferowany komputer przenośny musi osiągać w teście wydajności :SysMark25– wynik min. 600 pkt – test z przeprowadzonej konfiguracji na wezwanie Zamawiającego załączyć do oferty.Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS ( tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.).Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów Oferent musi dostarczyć Zamawiającemu 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 |
| Pamięć operacyjna | Min 8GB z możliwością rozbudowy do 16GB, rodzaj pamięci min. DDR4. |
| Dysk twardy | Min. 256GB SSD M.2 zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.Możliwość instalacji dwóch dysków twardych w obudowie komputera. |
| Karta graficzna | Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia do 2 GB pamięci.Karta graficzna osiągająca w teście SysMark25 Creativity wynik min. 550 pkt. – test z przeprowadzonej konfiguracji na wezwanie Zamawiającego załączyć do oferty. |
| Audio/Video | Wbudowana, zgodna z HD Audio, wbudowane głośniki stereo min 2x 2W, wbudowany mikrofon, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute), wbudowana kamera 720p. |
| Karta sieciowa | Zintegrowana z płytą główną 10/100/1000 – RJ45 |
| Porty/złącza | 3xUSB w tym minimum 2xUSB 3.2, złącze słuchawek i złącze mikrofonu typu COMBO, 1xHDMI, RJ-45. Złącze bezpieczeństwa typu Kensington lub Noble. |
| Klawiatura | Klawiatura wyspowa, układ US. Klawiatura z wydzielonym blokiem numerycznym. |
| WiFi | Wbudowana karta sieciowa, pracująca w standardzie AC |
| Bluetooth | Wbudowany moduł Bluetooth 4.2 |
| Bateria | Bateria pojemności min. 35Whr. Umożliwiająca jej szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin.Czas pracy na baterii mi. 8 godzin, potwierdzony przeprowadzonym testem MobileMark 25 Battery Life [do oferty załączyć wydruk przeprowadzonego testu lub link publikacji na stronie BAPCO, w oferowanej konfiguracji] |
| Zasilacz | Zewnętrzny w wersji niewymagającej przejściówek. Europejska wersja zasilania.Dostosowany mocą do urządzenia. |
| BIOS | BIOS zgodny ze specyfikacją UEFI. Możliwość odczytania z BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych następujących informacji: - wersji BIOS - nr seryjnym komputera- ilości pamięci RAM- typie procesora i jego prędkości-modele zainstalowanych dysków twardychAdministrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności:Możliwość ustawienia hasła dla twardego dyskuMożliwość ustawienia hasła na starcie komputera tzw. POWER-On PasswordMożliwość ustawienia hasła Administratora i użytkownika BIOSMożliwość włączania/wyłączania wirtualizacji z poziomu BIOSUMożliwość Wyłączania/Włączania: zintegrowanej karty WIFI, portów USB,Tryby 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.System diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub z poziomu menu boot, umożliwiający przetestowanie komponentów komputera. Pełna funkcjonalność systemu diagnostycznego musi być realizowana bez użycia : dostępu do sieci i internetu, dysku twardego również w przypadku jego braku, urządzeń zewnętrznych i wewnętrznych typu : pamięć flash, USBpen itp.  |
| Bezpieczeństwo | złącze Kensington Lock,- 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 2.0).Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu powoduje uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej.Zainstalowane oprogramowanie :Backup i przywracanie danych- Deduplikacja danych na źródle,- Backup przyrostowy i różnicowy,- Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji,- Backup danych lokalnych – plikowy oraz poczty Outlook,- Backup otwartych plików (VSS),- Filtr plików oraz folderów,- Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.),- Wyłączanie komputera po wykonaniu backupu,- Przywracanie danych do wskazanej lokalizacji,- Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora,- Wyszukiwanie plików w repozytorium użytkownika,Ustawienia- Automatyczne logowanie,- Zapamiętywanie danych logowania,- Automatyczne uruchamianie programu przy starcie systemu,- Ustawianie priorytetu dla procesu backupu,- Zmiana klucza szyfrującego,- Ustawienia przepustowości/zajętości pasma,- Konfiguracja wydajności procesu backupu,Bezpieczeństwo- Zastępowanie nazwy pliku GUID-em,- Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika,- Kompresja danych,- Transmisja po bezpiecznym protokole TLS,- Deklaracja klucza szyfrującego dane użytkownika,- Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji,- Obliczanie sumy kontrolnej,- Kopie zapasowe są przechowywane w profesjonalnych, certyfikowanych data center, na terenie Polski.WSPIERANE SYSTEMY OPERACYJNE Microsoft Windows 7 i nowsze, Mac OS, Licencje przypisywane do jednego urządzenia z limitem pojemności przestrzeni w chmurze – minimum 50 GB. Licencja obowiązuje minimum przez okres gwarancji laptopa. Wsparcie techniczne, świadczone jest bezpośrednio od producenta, w języku polskim, zawarte jest w cenie licencji. |
| Certyfikaty i standardy | Certyfikat ISO 9001 oraz ISO 50 001 dla producenta sprzętu (należy załączyć do oferty)ENERGY STAR - certyfikat lub wydruk ze strony http://www.eu-energystar.org lub http://www.energystar.govDeklaracja zgodności CE (załączyć do oferty) |
| Waga/Wymiary | Waga urządzenia z baterią podstawową maksymalnie 1,9kg |
| System operacyjny – w formularzu oferty trzeba podać nazwę oferowanego oprogramowania | Minimum Windows 10 Home 64 bit lub równoważny\*System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim9. Wbudowany system pomocy w języku polskim.10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.Klucz produktu przypisany do komputera aby przy ponownej reinstalacji systemu nie było konieczności wpisywania klucza. |
| Oprogramowanie antywirusowe | 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.• 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 wrażliwościSzyfrowanie 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.podłączanych do stacji końcowej.Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej.Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną anty ransomware.Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware• Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracjiZarządzanie przez Chmurę:1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznejWspierane platformy i systemy operacyjne:1. Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit)2. Mac OS X, Mac OS 103. Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHatPlatforma do zarządzania dla Android i iOS:• Musi zapewnić kompleksowy system ochrony i zarządzania urządzeniami mobilnymi z systemami Android oraz iOS a także ich ochronę• Funkcjonalność musi być realizowana za pomocą platformy w chmurzeZarządzanie użytkownikiemOprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa:Wymagania dotyczące technologii:1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta.3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych:Microsoft Internet Explorer , Microsoft Edge, Mozilla Firefox, Google Chrome,- Safari4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących5. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie |
| Gwarancja | 2-letnia gwarancja(24 miesiące), czas reakcji serwisu, do końca następnego dnia roboczego. Gwarancja musi oferować przez cały okres :- mieć opiekę kierownika technicznego ds. Eskalacji dostępność wsparcia technicznego przez 7 dni w tygodniu przez cały rok w dni robocze (w języku polskim w dni robocze)Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera. |

**\*Opis równoważności dla systemu operacyjnego:**

System operacyjny fabrycznie przeinstalowany przez producenta klas y desktop musi spełniać

następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:

a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,

b) Dotykowy umożliwiający s terowanie dotykiem na urządzeniach typu tablet lub

monitorach dotykowych.

2. Interfejsy użytkownika dostępne w wielu językach do wyboru w tym Polskim i Angielskim.

3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe.

4. Wbudowany system pomocy w języku polskim.

5. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim.

6. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika obsługa języka polskiego.

7. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika.

8. 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.

9. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.

10. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.

11. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych;

zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.

12. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.

13. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi Fi).

14. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer.

15. Możliwość zarządzania stacją roboczą poprzez polityki grupowe przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji.

16. Rozbudowane, definiowalne polityki bezpieczeństwa polityki dla systemu operacyjnego i dla wskazanych aplikacji.

17. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania

systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe.

18. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.

19. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu.

20. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych.

21. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.

22. Obsługa standardu NFC (near field communication).

23. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).

24. Wsparcie dla IPSEC oparte na politykach wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.

25. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.

26. Mechanizmy logowania do domeny w oparciu o:

a) Login i hasło,

b) Karty z certyfikatami (smartcard),

c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).

27. Mechanizmy wieloelementowego uwierzytelniania.

28. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5.

29. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu.

30. Wsparcie dla algorytmów Suite B (RFC 4869).

31. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec.

32. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk.

33. Wsparcie dla środowisk Java i .NET Framework 4.x możliwość uruchomienia aplikacji działających we wskazanych środowiskach.

34. Wsparcie dla JScript i VBScript możliwość uruchamiania interpretera poleceń.

35. Zdalna pomoc i współdzielenie aplikacji możliwość zdalnego prze jęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.

36. 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.

37. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację.

38. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.

39. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.

40. Udostępnianie modemu.

41. Oprogramowanie dla tworzenia kopii zapasowych (Backup ); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.

42. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.

43. 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.).

44. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).

45. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie

z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych.

46. Mechanizm szyfrowania dysk ów wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika.

47. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module)w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB.

48. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych.

49. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.

50. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.