ZAŁĄCZNIK NR 1a DO SIWZ

Znak sprawy: 1/271/2018

Województwo Lubuskie- Centrum Kształcenia Zawodowego i Ustawicznego „MEDYK” w Gorzowie Wielkopolskim

Opis Przedmiotu Zamówienia

Dostawa sprzętu komputerowego wraz z oprogramowaniem w ramach projektu „Poprawa warunków edukacyjnych w Centrum Kształcenia Zawodowego i Ustawicznego „Medyk” w Gorzowie Wlkp.” **Program Operacyjny – Lubuskie 2020 Osi Priorytetowej 9 Infrastruktura społeczna** dla Działania **9.3 Rozwój infrastruktury edukacyjnej** dla Poddziałania **9.3.1 Rozwój infrastruktury edukacyjnej – projekty realizowane poza formułą ZIT**

1. **Zestaw komputerowy wraz z oprogramowaniem - 16 sztuk**

a) Stacja komputerowa

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
1	Zastosowanie	Komputer stacjonarny, który będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej. W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
2	Niezawodność	Komputer przystosowany do pracy ciągłej 24/7
3	Wydajność	Procesor powinien osiągać w teście wydajności PassMark PerformanceTest (wynik dostępny: https://www.cpubenchmark.net/high_end_cpus.html) co najmniej wynik 7300 punktów Passmark CPU Mark
4	Pamięć RAM	Pamięć operacyjna: 8 GB DDR4 2400 MHz możliwość rozbudowy do min 64 GB minimum trzy gniazda wolne na rozbudowę pamięci
5	Pamięć masowa	Parametry pamięci masowej: dysk o pojemności min. 256 GB w technologii SSD zainstalowany na złączu M.2 płyty głównej, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii bez dodatkowych nośników. Drugi dysk twardy SATA o pojemności min. 1TB i prędkości 7200 obr./min. Dyski zainstalowane przez producenta na etapie produkcji komputera.
6	Karta graficzna	Wydajność grafiki: Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia do 1,5 GB pamięci. Obsługująca funkcje: DirectX 12, OpenGL 4.4, OpenCL 2.1, HLSL shader model 5.1
7	Zdalne zarządzanie	Wbudowana w płytę główną technologia monitorowania i zarządzania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6 zapewniająca funkcjonalność Intel Standard Manageability lub technologii równoważnej.
8	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji.
9	Bezpieczeństwo	Sprzętowe wsparcie technologii weryfikacji poprawności podpisu cyfrowego wykonywanego kodu oprogramowania, oraz sprzętowa izolacja segmentów pamięci dla kodu wykonywanego w trybie zaufanym wbudowane w procesor, kontroler pamięci, chipset I/O. Złącze typu Kensington Lock lub równoważne, 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. Co najmniej TPM 2.0.
10	Multimedia	Wyposażenie multimedialne: Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition audio i obsługująca 5.1 surround sound. Porty słuchawek i mikrofonu wymagane zarówno na przednim, jak i na tylnym panelu obudowy. Wbudowany w obudowie komputera głośnik umożliwiający odtwarzanie dźwięków systemu oraz multimediów.
11	Klawiatura i mysz	Klawiatura USB w układzie QWERTY US min. 105 klawiszy. Mysz USB z trzema klawiszami oraz rolką (scroll) min 800dpi.
12	Zasilanie	Zasilacz o mocy minimum 280W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 94%, przy obciążeniu 50%.
13	Wymiary	Suma wymiarów obudowy (wysokość + szerokość + głębokość mierzona po krawędziach zewnętrznych) nie może wynosić więcej niż 862mm.
14	Obudowa	Obudowa przystosowana do pracy w pionie. Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń i napędów bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych); Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych) oraz powinna posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym

		producenta komputera. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej, kłódki (oczko w obudowie do założenia kłódki) oraz zamka nie wystającego poza linię obudowy. Obudowa typu mini tower z obsługą kart PCI Express wyłącznie o pełnym profilu, wyposażona w min. 6 kieszeni: 2 szt. 5,25" zewnętrzne w tym co najmniej jedna pełnowymiarowa i co najmniej jedna typu SLIM, 2 szt. 3,5" wewnętrzne, 1 szt. 3,5" zewnętrzna oraz 1 szt. 2,5" wewnętrzna" . 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.
15	Certyfikaty	Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z systemem operacyjnym Windows 10 Professional 64-bit (załączyć wydruk ze strony Microsoft WHCL) oraz Windows 10 Home 64-bit. Deklaracja zgodności CE lub równoważne (załączyć do oferty) Norma EnergyStar 6.1- komputer musi znajdować się na liście zgodności dostępnej na stronie www.energystar.gov oraz http://www.eu-energystar.org Oferowane laptopy muszą być wykonane/wyprodukowane w systemie zapewnienia jakości ISO 9001 i ISO 14001 – certyfikat należy załączyć do oferty. Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie jałowym (IDLE) wynosząca maksymalnie 20dB (załączyć oświadczenie producenta i/lub raport z pomiarów głośności). Wylot powietrza chłodzącego notebooka z tyłu obudowy – brak otworów wentylacyjnych na bokach obudowy. Zamawiający wymaga dodatkowo: o 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). o 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
16	BIOS	Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: - modelu komputera; - modelu płyty głównej; - nr seryjnego komputera; - wersji BIOS (z datą); - modelu procesora wraz z informacjami o prędkości taktowania; - Informacji o ilości i obsadzeniu slotów pamięci RAM wraz z informacją o prędkości taktowania; - Informacji o dysku twardym: model oraz pojemność - MAC adresie zintegrowanej karty sieciowej - temperaturze układu graficznego - temperaturze procesora - temperaturze wewnątrz obudowy komputera - prędkości obrotowej wentylatora - statusu karty sieciowej Możliwość wyłączenia/włączenia bez uruchamiania systemu operacyjnego z dysku twardego

		komputera lub innych, podłączonych do niego, urządzeń zewnętrznych min.: - karty sieciowej RJ45 - karty dźwiękowej - portów szeregowych z możliwością ustawienia trybu pracy - portu równoległego z możliwością ustawienia trybu pracy - sprzętowego wsparcia wirtualizacji - wsparcia wirtualizacji Directed I/O - funkcji regulacji częstotliwości taktowania CPU w zależności od obciążenia (Enhanced SpeedStep) - funkcji Turbo Mode pozwalającej logicznym procesorom CPU osiągać wyższe częstotliwości taktowania od domyślnych w sytuacji gdy pozwalają na to termiczne parametry pracy procesora - kontrolera SATA zarówno w całości jak i z możliwością pojedynczego wyłączania poszczególnych portów SATA oraz M.2 SATA - funkcji SMART - funkcji automatycznego zarządzania głośnością pracy napędów optycznych i dysków - modułu TPM - portów USB w tym: włączenia wszystkich portów, wyłączenia wszystkich portów, włączenia jedynie przednich i wewnętrznych, włączenia jedynie tylnych i wewnętrznych, włączenia jedynie wewnętrznych, włączenia jedynie używanych (system sprawdza przy starcie komputera, w których portach USB jest włączone urządzenie i tylko te aktywuje) - funkcji blokowania portów USB w tym: włączenia wszystkich portów, włączenia jedynie portów do których podłączono klawiaturę i mysz, włączenia wszystkich portów za wyjątkiem portów do których podłączono USB hub lub zewnętrzną pamięć masową. - funkcji Wake-on-LAN Możliwość ustawienia bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych min.: - liczby aktywnych rdzeni procesora - funkcji sterowania prędkością wentylatorów w komputerze w co najmniej trzech trybach: Automatycznym, trybie zwiększonej przepływności powietrza w celu osiągnięcia maksymalnej wydajności procesora, trybie maksymalnej wydajności wszystkich wentylatorów. - trybu pracy karty sieciowej - 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 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 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-z z częstotliwością co najmniej: raz dziennie, raz na tydzień, raz na miesiąc i raz na kwartał. Funkcja blokowania/odblokowania BOOT-owania z dysku twardego, zewnętrznych urządzeń oraz sieci bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z USB. Możliwość włączenia/wyłączenia hasła dla dysku twardego. Możliwość - bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych - ustawienia hasła na poziomie użytkownika, administratora i dysku twardego oraz możliwość ustawienia co najmniej dwóch rodzajów haseł: hasło standardowe, które może zostać skasowane za pomocą zworki na płycie głównej komputera oraz hasło silne, którego skasowanie jest możliwe jedynie poprzez interwencję serwisu producenta komputera. Musi posiadać możliwość ustawienia zależności pomiędzy hasłem administratora a hasłem użytkownika tak, aby nie było możliwe wprowadzenie zmian w BIOS wyłącznie po podaniu hasła użytkownika. Funkcja ta ma wymuszać podanie hasła administratora przy próbie zmiany ustawień BIOS w sytuacji, gdy zostało podane hasło użytkownika.
17	Dodatkowe oprogramowanie	Oprogramowanie dostarczone przez producenta komputera (lokalny agent na maszynie) pozwalające na zdalną inwentaryzację komputerów w sieci, lokalną i zdalną inwentaryzację

		komponentów komputera, umożliwiające co najmniej: - Zdalne wyłączanie, 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 indywidualnych numerów dla poszczególnych użytkowników, - Włączenie lub wyłączanie BOOTowania portów USB Oprogramowanie umożliwiające w pełni automatyczną instalację sterowników urządzeń opartą o automatyczną detekcję posiadanego sprzętu.
18	System operacyjny	Zainstalowany system operacyjny w wersji licencyjnej dla Edukacji (licencja bez ograniczeń czasowych) – o ile będzie to możliwe, niewymagający aktywacji za pomocą telefonu lub Internetu. Dołączony nośnik Recovery umożliwiający instalacje systemu w wersji 64 bitowej. System operacyjny klasy desktop musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Interfejs graficzny użytkownika pozwalający na obsługę: a. Klasyczną przy pomocy klawiatury i myszy, b. Dotykową umożliwiającą sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych, 2. Interfejsy użytkownika dostępne w wielu językach do wyboru w czasie instalacji – w tym Polskim i Angielskim, 3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, klient poczty elektronicznej z kalendarzem spotkań, pomoc, komunikaty systemowe, 4. Wbudowany mechanizm pobierania map wektorowych z możliwością wykorzystania go przez zainstalowane w systemie aplikacje, 5. Wbudowany system pomocy w języku polskim; 6. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim, 7. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego. 8. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika. 9. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta z mechanizmem sprawdzającym, które z poprawek są potrzebne, 10. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego, 11. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego, 12. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; 13. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami, 14. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi), 15. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer, 16. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji, 17. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji, 18. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe, 19. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 20. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego

		systemu. 21. 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, 22. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. 23. Obsługa standardu NFC (near field communication), 24. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); 25. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; 26. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509; 27. Mechanizmy uwierzytelniania w oparciu o: a. Login i hasło, b. Karty z certyfikatami (smartcard), c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Wirtualnej tożsamości użytkownika potwierdzanej za pomocą usług katalogowych i konfigurowanej na urządzeniu. Użytkownik loguje się do urządzenia poprzez PIN lub cechy biometryczne, a następnie uruchamiany jest proces uwierzytelnienia wykorzystujący link do certyfikatu lub pary asymetrycznych kluczy generowanych przez moduł TPM. Dostawcy tożsamości wykorzystują klucz publiczny, zarejestrowany w usłudze katalogowej do walidacji użytkownika poprzez jego mapowanie do klucza prywatnego i dostarczenie hasła jednorazowego (OTP) lub inny mechanizm, jak np. telefon do użytkownika z żądaniem PINu. Mechanizm musi być ze specyfikacją FIDO. 28. Mechanizmy wieloskładnikowego uwierzytelniania. 29. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5, 30. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu, 31. Wsparcie dla algorytmów Suite B (RFC 4869) 32. Mechanizm ograniczający możliwość uruchamiania aplikacji tylko do podpisanych cyfrowo (zaufanych) aplikacji zgodnie z politykami określonymi w organizacji, 33. Funkcjonalność tworzenia list zabronionych lub dopuszczonych do uruchamiania aplikacji, możliwość zarządzania listami centralnie za pomocą polityk. Możliwość blokowania aplikacji w zależności od wydawcy, nazwy produktu, nazwy pliku wykonywalnego, wersji pliku 34. Izolacja mechanizmów bezpieczeństwa w dedykowanym środowisku wirtualnym, 35. Mechanizm automatyzacji dołączania do domeny i odłączania się od domeny, 36. Możliwość zarządzania narzędziami zgodnymi ze specyfikacją Open Mobile Alliance (OMA) Device Management (DM) protocol 2.0, 37. Możliwość selektywnego usuwania konfiguracji oraz danych określonych jako dane organizacji, 38. Możliwość konfiguracji trybu „kioskowego" dającego dostęp tylko do wybranych aplikacji i funkcji systemu, 39. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec, 40. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; 41. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach, 42. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń, 43. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem, 44. Mechanizm pozwalający na dostosowanie konfiguracji systemu dla wielu użytkowników w organizacji bez konieczności tworzenia obrazu instalacyjnego. (provisioning) 45. 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, 46. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację, 47. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe, 48. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe 49. Udostępnianie wbudowanego modemu, 50. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej, 51. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci, 52. 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.), 53. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu), 54. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych, 55. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika, 56. 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. 57. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych 58. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych. 59. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.
19	Porty i złącza	- 1 x DVI - 2 x Display Port 1.2 - 1 x RS-232 zintegrowane z płytą główną - 2 x PS/2 - 1 x Audio: line-in - 1 x Audio: line-out - 1 x Audio: mikrofon z przodu obudowy - 1 x Audio: słuchawki z przodu obudowy - 13 szt. USB w tym: minimum 5 portów z przodu obudowy (w tym min. 2 x USB 3.0 oraz min. 1x USB 3.1 Type C Gen1), minimum 6 portów z tyłu obudowy (w tym min. 4 x USB 3.0), minimum 2 porty wewnątrz obudowy. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. o Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika) o 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) o Płyta główna z wbudowanymi: - 2 złącza PCI-Express x1 - 1 złącze PCI-Express 2.0 x4 (mech. x16) - 1 złącze PCI-Express 3.0 x16 - 1 złącze M.2-2280 umożliwiający zamontowanie modułu PCIe lub dysku SSD. Złącze musi obsługiwać Intel Optane Technology Obsługa kart rozszerzeń wyłącznie o pełnym profilu.

		Minimum cztery złącza DIMM z obsługą do 64 GB DDR4 pamięci RAM, min. 5 złączy SATA 3.0 (6 Gbit) NCQ w tym min 2 złącza eSATA, Nagrywarka DVD +/-RW o Zintegrowany w obudowie czytnik kart multimedialnych 24in1 wyposażony w diody sygnalizacyjne (praca, obecność karty, odczyt) o Z tyłu obudowy osłona na kable
20	Gwarancja	Gwarancja jakości producenta: o 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, o Czas reakcji na zgłoszoną reklamację gwarancyjną - do końca następnego dnia roboczego, o W przypadku naprawy trwającej dłużej niż 48 godzin, zamawiającemu musi zostać dostarczony komputer zastępczy, o Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta, o w celu zapewnienia prawidłowej realizacji gwarancji w całym okresie użytkowania zamawiający wymaga oświadczenia producenta komputera że w razie nie wywiązywania się oferenta Producent przejmie wskazane w wymaganiach obowiązki gwarancyjne Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela
21	Pakiet biurowy	Pakiet biurowy - oprogramowanie w wersji licencyjnej dla Edukacji (licencja bez ograniczeń czasowych), musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępność pakietu w wersjach 32-bit oraz 64-bit umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej, 2. Wymagania odnośnie interfejsu użytkownika: a. Pełna polska wersja językowa interfejsu użytkownika z możliwością przełączania wersji językowej interfejsu na inne języki, w tym język angielski. b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych. c. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się. 3. Możliwość aktywacji zainstalowanego pakietu poprzez mechanizmy wdrożonej usługi katalogowej Active Directory. 4. Narzędzie wspomagające procesy migracji z poprzednich wersji pakietu i badania zgodności z dokumentami wytworzonymi w pakietach biurowych. 5. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym standardzie, który spełnia następujące warunki: a. posiada kompletny i publicznie dostępny opis formatu, b. ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012, poz. 526), c. umożliwia kreowanie plików w formacie XML, d. wspiera w swojej specyfikacji podpis elektroniczny w formacie XAdES, 6. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji. 7. Oprogramowanie musi umożliwiać opatrywanie dokumentów metadanymi. 8. W skład oprogramowania muszą wchodzić narzędzia programistyczne

		umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy). 9. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim. 10. Pakiet zintegrowanych aplikacji biurowych musi zawierać: a. Edytor tekstów b. Arkusz kalkulacyjny c. Narzędzie do przygotowywania i prowadzenia prezentacji d. Narzędzie do tworzenia drukowanych materiałów informacyjnych e. Narzędzie do tworzenia i pracy z lokalną bazą danych f. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) g. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR. h. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video. 11. Edytor tekstów musi umożliwiać: a. 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. b. Edycję i formatowanie tekstu w języku angielskim wraz z obsługą języka angielskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty. c. Wstawianie oraz formatowanie tabel. d. Wstawianie oraz formatowanie obiektów graficznych. e. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne). f. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków. g. Automatyczne tworzenie spisów treści. h. Formatowanie nagłówków i stopek stron. i. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie. j. Zapamiętywanie i wskazywanie miejsca, w którym zakończona była edycja dokumentu przed jego uprzednim zamknięciem. k. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. l. Określenie układu strony (pionowa/pozioma). m. Wydruk dokumentów. n. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną. o. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2010, 2013 i 2016 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu. p. Zapis i edycję plików w formacie PDF. q. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. r. Możliwość jednoczesnej pracy wielu użytkowników na jednym dokumencie z uwidacznianiem ich uprawnień i wyświetlaniem dokonywanych przez nie zmian na bieżąco, s. Możliwość wyboru jednej z zapisanych wersji dokumentu, nad którym pracuje wiele osób. 12. Arkusz kalkulacyjny musi umożliwiać: a. Tworzenie raportów tabelarycznych b. Tworzenie wykresów liniowych (wraz linią 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 edycję 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. Tworzenie wykresów prognoz i trendów na podstawie danych historycznych z użyciem algorytmu ETS j. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie k. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności l. Formatowanie czasu, daty i wartości finansowych z polskim formatem m. Zapis wielu arkuszy kalkulacyjnych w jednym pliku. n. Inteligentne uzupełnianie komórek w kolumnie według rozpoznanych wzorców, wraz z ich możliwością poprawiania poprzez modyfikację proponowanych formuł. o. Możliwość przedstawienia różnych wykresów przed ich finalnym wyborem (tylko po najechaniu znacznikiem myszy na dany rodzaj wykresu). p. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2010, 2013 i 2016, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń. q. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji 13. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: a. Przygotowywanie prezentacji multimedialnych, które będą: i. Prezentowanie przy użyciu projektora multimedialnego ii. Drukowanie w formacie umożliwiającym robienie notatek b. Zapisanie jako prezentacja tylko do odczytu. c. Nagrywanie narracji i dołączanie jej do prezentacji d. Opatrywanie slajdów notatkami dla prezentera e. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo f. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego g. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym h. Możliwość tworzenia animacji obiektów i całych slajdów i. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, z możliwością podglądu następnego slajdu. j. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2010, 2013 i 2016. 14. Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać: a. Tworzenie i edycję drukowanych materiałów informacyjnych b. Tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów. c. Edycję poszczególnych stron materiałów. d. Podział treści na kolumny. e. Umieszczanie elementów graficznych. f. wykorzystanie mechanizmu korespondencji seryjnej

		g. Płynne przesuwanie elementów po całej stronie publikacji. h. Eksport publikacji do formatu PDF oraz TIFF. i. Wydruk publikacji. j. Możliwość przygotowywania materiałów do wydruku w standardzie CMYK. 15. Narzędzie do tworzenia i pracy z lokalną bazą danych musi umożliwiać: a. Tworzenie bazy danych przez zdefiniowanie: b. Tabel składających się z unikatowego klucza i pól różnych typów, w tym tekstowych i liczbowych. c. Relacji pomiędzy tabelami d. Formularzy do wprowadzania i edycji danych e. Raportów f. Edycję danych i zapisywanie ich w lokalnie przechowywanej bazie danych g. Tworzenie bazy danych przy użyciu zdefiniowanych szablonów h. Połączenie z danymi zewnętrznymi, a w szczególności z innymi bazami danych zgodnymi z ODBC, plikami XML, arkuszem kalkulacyjnym. 16. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: a. Uwierzytelnianie wieloskładnikowe poprzez wbudowane wsparcie integrujące z usługą Active Directory, b. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, c. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych, d. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców, e. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, f. Automatyczne grupowanie poczty o tym samym tytule, g. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy, h. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów, i. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie, j. Zarządzanie kalendarzem, k. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników, l. Przeglądanie kalendarza innych użytkowników, m. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach, n. Zarządzanie listą zadań, o. Zlecanie zadań innym użytkownikom, p. Zarządzanie listą kontaktów, q. Udostępnianie listy kontaktów innym użytkownikom, r. Przeglądanie listy kontaktów innych użytkowników, s. Możliwość przesyłania kontaktów innym użytkowników, t. Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http. 17. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video musi spełniać następujące wymagania: a. Pełna polska wersja językowa interfejsu użytkownika. b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych. c. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o

		ponowne uwierzytelnienie się. d. Możliwość obsługi tekstowych wiadomości błyskawicznych. e. Możliwość komunikacji głosowej i video. f. Sygnalizowanie statusu dostępności innych użytkowników serwera komunikacji wielokanałowej. g. Możliwość definiowania listy kontaktów lub dołączania jej z listy zawartej w usłudze katalogowej. h. Możliwość wyświetlania szczegółowej informacji opisującej innych użytkowników oraz ich dostępność, pobieranej z usługi katalogowej i systemu kalendarzy serwera poczty elektronicznej.

b) monitor

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
1.	Przekątna ekranu	Min. 21,5”; 54,7cm
2.	Format obrazu	16:9
3.	Rozdzielczość fizyczna	Full HD, 1920x1080 pikseli @75Hz (2.1 megapixela)
4.	Jasność	250 cd/m^2
5.	Kontrast	3000:1
6.	Kontrast dynamiczny	80 000 000:1 ACR
7.	Czas reakcji matrycy	4 ms
8.	Kąty widzenia	Poziomo/pionowo: 178/178 stopni, prawo/lewo: 89/89 stopni, góra/dół 89/89 stopni
9.	Wyświetlane kolory	16,7 mln
10.	Redukcja niebieskiego światła	Tak
11.	Plamka matrycy	0,248 mm
12.	Częstotliwość pozioma	30-80 kHz
13.	Częstotliwość pionowa	55-75 Hz
14.	Wejścia sygnałowe	1x D-Sub (VGA), 1x HDMI, 1x DisplayPort
15.	Głośniki	Wbudowane 2x1W, dodatkowe wyjście słuchawkowe
16.	Kąty pochylenia	22 stopnie w górę, 5 stopni w dół
17.	Standard VESA	100x100
18.	Zasilacz	Wewnętrzny, AC 100-240V, 50/60Hz
19.	Zużycie energii	Typowa 21W
20.	Dołączone akcesoria	Kabel zasilający, kabel HDMI, kabel DisplayPort
21.	Gwarancja producenta	3 lata na monitor, 30 dni gwarancja producenta 0 pixeli/subpixeli
22.	Certyfikaty	CE, ISO 9001 i 14001 dla producenta, TCO 6.0 lub równoważny

2. Laptop - 2 sztuki

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
1	Przekątna ekranu	15,6” o rozdzielczości min. 1366x768 pikseli, powierzchnia ekranu matowa, antyrefleksyjna
2	Procesor	wydajność wg testów Passmark CPU Benchmark min. 3120 pkt. Wyniki opublikowane na stronie www.cpubenchmark.net. Do oferty dołączyć wydruk ze strony potwierdzający spełnianie tego warunku.
3	Pamięć RAM	min. 8GB RAM DDR4, 2 banki na pamięć RAM w tym jeden wolny do dalszej rozbudowy
4	Dysk twardy	pojemność min. 256GB SSD SATA, zawierający partycje Recovery umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii bez dodatkowych nośników
5	Napęd optyczny	Wbudowany napęd DVD +/-RW
6	Komunikacja	WiFi 802.11 a/b/g/n/ac, Bluetooth, LAN 10/100/1000 Mbit/s
7	Multimedia	karta muzyczna zgodna z HD Audio, wbudowany mikrofon i głośniki,

		wbudowana kamera i czytnik kart
8	Porty USB	min. 2xUSB 3.0, min. 1xUSB 2.0
9	Porty video	1xHDMI, 1xVGA
10	Bateria	Litowo-Jonowa, min. 4-komorowa
11	Zasilacz	moc max. 45W
12	Waga	Max. 2,25kg
13	Gwarancja	3 lata, czas reakcji w następnym dniu roboczym, naprawa w miejscu instalacji
14	Certyfikaty	CE, ISO dla producenta sprzętu
15	System operacyjny	System operacyjny w wersji licencyjnej dla Edukacji (licencja bez ograniczeń czasowych) – o ile będzie to możliwe, klasy desktop musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Interfejs graficzny użytkownika pozwalający na obsługę: a. Klasyczną przy pomocy klawiatury i myszy, b. Dotykową umożliwiającą sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych, 2. Interfejsy użytkownika dostępne w wielu językach do wyboru w czasie instalacji – w tym Polskim i Angielskim, 3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, klient poczty elektronicznej z kalendarzem spotkań, pomoc, komunikaty systemowe, 4. Wbudowany mechanizm pobierania map wektorowych z możliwością wykorzystania go przez zainstalowane w systemie aplikacje, 5. Wbudowany system pomocy w języku polskim; 6. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim, 7. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego. 8. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika. 9. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta z mechanizmem sprawdzającym, które z poprawek są potrzebne, 10. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego, 11. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego, 12. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; 13. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami, 14. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi), 15. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer, 16. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji, 17. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji,

		18. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe, 19. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 20. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu. 21. 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, 22. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. 23. Obsługa standardu NFC (near field communication), 24. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); 25. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; 26. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509; 27. Mechanizmy uwierzytelniania w oparciu o: a. Login i hasło, b. Karty z certyfikatami (smartcard), c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Wirtualnej tożsamości użytkownika potwierdzanej za pomocą usług katalogowych i konfigurowanej na urządzeniu. Użytkownik loguje się do urządzenia poprzez PIN lub cechy biometryczne, a następnie uruchamiany jest proces uwierzytelnienia wykorzystujący link do certyfikatu lub pary asymetrycznych kluczy generowanych przez moduł TPM. Dostawcy tożsamości wykorzystują klucz publiczny, zarejestrowany w usłudze katalogowej do walidacji użytkownika poprzez jego mapowanie do klucza prywatnego i dostarczenie hasła jednorazowego (OTP) lub inny mechanizm, jak np. telefon do użytkownika z żądaniem PINu. Mechanizm musi być ze specyfikacją FIDO. 28. Mechanizmy wieloskładnikowego uwierzytelniania. 29. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5, 30. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu, 31. Wsparcie dla algorytmów Suite B (RFC 4869) 32. Mechanizm ograniczający możliwość uruchamiania aplikacji tylko do podpisanych cyfrowo (zaufanych) aplikacji zgodnie z politykami określonymi w organizacji, 33. Funkcjonalność tworzenia list zabronionych lub dopuszczonych do uruchamiania aplikacji, możliwość zarządzania listami centralnie za pomocą polityk. Możliwość blokowania aplikacji w zależności od wydawcy, nazwy produktu, nazwy pliku wykonywalnego, wersji pliku 34. Izolacja mechanizmów bezpieczeństwa w dedykowanym środowisku wirtualnym, 35. Mechanizm automatyzacji dołączania do domeny i odłączania się od domeny, 36. Możliwość zarządzania narzędziami zgodnymi ze specyfikacją Open Mobile Alliance (OMA) Device Management (DM) protocol

		2.0, 37. Możliwość selektywnego usuwania konfiguracji oraz danych określonych jako dane organizacji, 38. Możliwość konfiguracji trybu „kioskowego" dającego dostęp tylko do wybranych aplikacji i funkcji systemu, 39. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec, 40. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; 41. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach, 42. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń, 43. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem, 44. Mechanizm pozwalający na dostosowanie konfiguracji systemu dla wielu użytkowników w organizacji bez konieczności tworzenia obrazu instalacyjnego. (provisioning) 45. 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, 46. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację, 47. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe, 48. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe 49. Udostępnianie wbudowanego modemu, 50. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej, 51. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci, 52. 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.), 53. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu), 54. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych, 55. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika, 56. 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. 57. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania

		dysków przenośnych 58. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych. 59. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.
16	Pakiet biurowy	Pakiet biurowy - oprogramowanie w wersji licencyjnej dla Edukacji (licencja bez ograniczeń czasowych), musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępność pakietu w wersjach 32-bit oraz 64-bit umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej, 2. Wymagania odnośnie interfejsu użytkownika: a. Pełna polska wersja językowa interfejsu użytkownika z możliwością przełączania wersji językowej interfejsu na inne języki, w tym język angielski. b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych. c. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się. 3. Możliwość aktywacji zainstalowanego pakietu poprzez mechanizmy wdrożonej usługi katalogowej Active Directory. 4. Narzędzie wspomagające procesy migracji z poprzednich wersji pakietu i badania zgodności z dokumentami wytworzonymi w pakietach biurowych. 5. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym standardzie, który spełnia następujące warunki: a. posiada kompletny i publicznie dostępny opis formatu, b. ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012, poz. 526), c. umożliwia kreowanie plików w formacie XML, d. wspiera w swojej specyfikacji podpis elektroniczny w formacie XAdES, 6. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji. 7. Oprogramowanie musi umożliwiać opatrywanie dokumentów metadanymi. 8. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy). 9. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim. 10. Pakiet zintegrowanych aplikacji biurowych musi zawierać: a. Edytor tekstów

		b. Arkusz kalkulacyjny c. Narzędzie do przygotowywania i prowadzenia prezentacji d. Narzędzie do tworzenia drukowanych materiałów informacyjnych e. Narzędzie do tworzenia i pracy z lokalną bazą danych f. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) g. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR. h. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video. 11. Edytor tekstów musi umożliwiać: a. 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. b. Edycję i formatowanie tekstu w języku angielskim wraz z obsługą języka angielskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty. c. Wstawianie oraz formatowanie tabel. d. Wstawianie oraz formatowanie obiektów graficznych. e. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne). f. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków. g. Automatyczne tworzenie spisów treści. h. Formatowanie nagłówków i stopek stron. i. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie. j. Zapamiętywanie i wskazywanie miejsca, w którym zakończona była edycja dokumentu przed jego uprzednim zamknięciem. k. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. l. Określenie układu strony (pionowa/pozioma). m. Wydruk dokumentów. n. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną. o. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2010, 2013 i 2016 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu. p. Zapis i edycję plików w formacie PDF. q. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. r. Możliwość jednoczesnej pracy wielu użytkowników na jednym dokumencie z uwidacznianiem ich uprawnień i wyświetlaniem dokonywanych przez nie zmian na bieżąco, s. Możliwość wyboru jednej z zapisanych wersji dokumentu, nad którym pracuje wiele osób.

		12. Arkusz kalkulacyjny musi umożliwiać: a. Tworzenie raportów tabelarycznych b. Tworzenie wykresów liniowych (wraz linią 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 edycję 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. Tworzenie wykresów prognoz i trendów na podstawie danych historycznych z użyciem algorytmu ETS j. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie k. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności l. Formatowanie czasu, daty i wartości finansowych z polskim formatem m. Zapis wielu arkuszy kalkulacyjnych w jednym pliku. n. Inteligentne uzupełnianie komórek w kolumnie według rozpoznanych wzorców, wraz z ich możliwością poprawiania poprzez modyfikację proponowanych formuł. o. Możliwość przedstawienia różnych wykresów przed ich finalnym wyborem (tylko po najechaniu znacznikiem myszy na dany rodzaj wykresu). p. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2010, 2013 i 2016, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń. q. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji 13. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: a. Przygotowywanie prezentacji multimedialnych, które będą: i. Prezentowanie przy użyciu projektora multimedialnego ii. Drukowanie w formacie umożliwiającym robienie notatek b. Zapisanie jako prezentacja tylko do odczytu. c. Nagrywanie narracji i dołączanie jej do prezentacji d. Opatrywanie slajdów notatkami dla prezentera e. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo

		f. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego g. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym h. Możliwość tworzenia animacji obiektów i całych slajdów i. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, z możliwością podglądu następnego slajdu. j. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2010, 2013 i 2016. 14. Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać: a. Tworzenie i edycję drukowanych materiałów informacyjnych b. Tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów. c. Edycję poszczególnych stron materiałów. d. Podział treści na kolumny. e. Umieszczanie elementów graficznych. f. wykorzystanie mechanizmu korespondencji seryjnej g. Płynne przesuwanie elementów po całej stronie publikacji. h. Eksport publikacji do formatu PDF oraz TIFF. i. Wydruk publikacji. j. Możliwość przygotowywania materiałów do wydruku w standardzie CMYK. 15. Narzędzie do tworzenia i pracy z lokalną bazą danych musi umożliwiać: a. Tworzenie bazy danych przez zdefiniowanie: b. Tabel składających się z unikatowego klucza i pól różnych typów, w tym tekstowych i liczbowych. c. Relacji pomiędzy tabelami d. Formularzy do wprowadzania i edycji danych e. Raportów f. Edycję danych i zapisywanie ich w lokalnie przechowywanej bazie danych g. Tworzenie bazy danych przy użyciu zdefiniowanych szablonów h. Połączenie z danymi zewnętrznymi, a w szczególności z innymi bazami danych zgodnymi z ODBC, plikami XML, arkuszem kalkulacyjnym. 16. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: a. Uwierzytelnianie wieloskładnikowe poprzez wbudowane wsparcie integrujące z usługą Active Directory, b. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, c. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych, d. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i

		bezpiecznych nadawców, e. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, f. Automatyczne grupowanie poczty o tym samym tytule, g. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy, h. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów, i. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie, j. Zarządzanie kalendarzem, k. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników, l. Przeglądanie kalendarza innych użytkowników, m. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach, n. Zarządzanie listą zadań, o. Zlecanie zadań innym użytkownikom, p. Zarządzanie listą kontaktów, q. Udostępnianie listy kontaktów innym użytkownikom, r. Przeglądanie listy kontaktów innych użytkowników, s. Możliwość przesyłania kontaktów innym użytkowników, t. Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http. 17. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video musi spełniać następujące wymagania: a. Pełna polska wersja językowa interfejsu użytkownika. b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych. c. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się. d. Możliwość obsługi tekstowych wiadomości błyskawicznych. e. Możliwość komunikacji głosowej i video. f. Sygnalizowanie statusu dostępności innych użytkowników serwera komunikacji wielokanałowej. g. Możliwość definiowania listy kontaktów lub dołączania jej z listy zawartej w usłudze katalogowej. h. Możliwość wyświetlania szczegółowej informacji opisującej innych użytkowników oraz ich dostępność, pobieranej z usługi katalogowej i systemu kalendarzy serwera poczty elektronicznej.

3. Projektor multimedialny – 2 sztuki

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
1	Technologia	3LCD
2	Rozdzielczość	XGA (1024x768)
3	Jasność	min. 2700 ANSI lumenów
4	Współczynnik kontrastu	min. 2000:1
5	Głośność	max. 37dB (Normalna)
6	Żywotność lampy	min. 5000 godzin (Normalna)
7	Wielkość ekranu	30-300" (76-762cm)
8	Obiektyw	ręczny fokus, ręczny zoom x1,2
9	Proporcje	odległość : szerokość (:1): 1.5 (Wide) / 1.8 (Tele)
10	Głośnik	16Wx1 (mono)
11	Wejścia	HDMI (HDCP1.4 compilant), Mini D-sub 15-pin connector, RCA, stereo mini jack, 1 x para RCA, 1 x mikrofon, 9 pin D-sub dla sterowania przez RS-232C, USB typ B, RJ-45,
12	Wyjścia	15-pin mini D-sub, 3.5mm stereo mini jack
13	Gwarancja	3 lata na projektor, 3 lata gwarancji na lampę dla sektora edukacji

4. Tablica interaktywna wraz z projektorem multimedialnym ultrakrótkoogniskowym – 1 sztuka

a) Tablica interaktywna

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
1.	Powierzchnia	Efektywna powierzchnia tablicy (obszar interaktywny), na której można dokonywać notatek, sterować pracą komputera i wyświetlać obraz z projektora co najmniej 156 cm × 117 cm (przekątna 77 cali – 195 cm). Powierzchnia tablicy magnetyczna (wykorzystanie magnesów do mocowania kartek do tablicy) oraz umożliwiająca pisanie pisakami sucho ścieralnymi
2.	Format tablicy	4:3
3.	Waga	Max. 20kg
4.	Technologia	dotykowa, optyczna
5.	Komunikacja z komputerem	Komunikacja tablicy z komputerem za pomocą przewodu USB
6.	Gwarancja	2 lata, autoryzowany przez producenta tablicy serwis w Polsce, certyfikowany zgodnie z normą ISO 9001:2000 lub ISO 9001:2008 w zakresie urządzeń audiowizualnych
7.	Obsługa	Obsługa tablicy za pomocą załączonych pisaków i za pomocą palca. Półka na pisaki tego samego producenta co tablicy. W zestawie z tablicą dwa pisaki. Obsługa dwóch jednoczesnych dotknięć umożliwia pracę do dwóch użytkowników z materiałem interaktywnym na tablicy wykorzystując dołączone pisaki, inne przedmioty lub swoje palce do pisania. Rozpoznawanie gestów wielodotyku: dotknięcie obiektu w dwóch punktach i obracanie punktów dotyku wokół środka – obracanie obiektu, dotknięcie obiektu w dwóch punktach i oddalanie lub przybliżanie punktów dotyku – zwiększanie i zmniejszanie obiektu.
8.	Oprogramowanie interaktywne	Oprogramowanie do obsługi tablicy lub monitora interaktywnego (zwanych dalej interaktywny wyświetlacz), które pozwala na przygotowanie treści lekcji, jej wyświetlenie w czasie zajęć i archiwizację po ich zakończeniu. Wszystkie wyspecyfikowane funkcje musi posiadać jedno oferowane oprogramowanie. Wszystkie opisane poniżej funkcje muszą być realizowane bez konieczności wychodzenia lub minimalizowania programu. Nie dopuszcza się realizacji funkcji przez więcej niż jedno oprogramowanie. Multitouch (wielodotyk)

		• Program musi obsługiwać, co najmniej dwadzieścia równoczesnych dotknięć, kiedy jest używany z kompatybilnym interaktywnym wyświetlaczem wielodotykowym. • Aplikacja musi obsługiwać multituch (wielodotyk) w systemach operacyjnych Windows i MAC, gdy są one używane z kompatybilnym interaktywnym wyświetlaczem wielodotykowym. • Oprogramowanie musi obsługiwać gesty multitouch wykonywane przez jednego lub wielu użytkowników jednocześnie przy kompatybilnym interaktywnym wyświetlaczu wielodotykowym. • Program musi wspierać co najmniej gesty: o powiększanie i pomniejszanie obiektu poprzez zbliżanie i oddalanie palców dotykających go, o obracanie obiektu poprzez przesuwanie palców osiowo względem siebie, o przesuwanie palcem w lewo lub w prawo na pustym fragmencie strony w celu przejścia do kolejnie lub poprzedniej strony, o potrząśnięcie zaznaczonymi obiektami w celu ich zgrupowania lub potrząśniecie obiektem zgrupowanym w celu jego rozgrupowania na elementy składowe. <u>Tworzenie materiałów lekcyjnych</u> • Program do interaktywnych wyświetlaczy musi pozwalać na przygotowanie i prezentację treści lekcji lokalnie z dysku komputera. Nie dopuszczalne są rozwiązania zdalne, chmurowe dostępne poprzez sieć Internet. • Program do interaktywnych wyświetlaczy musi zawierać kreator do tworzenia ćwiczeń interaktywnych, który pozwala nauczycielom wybierać spośród zestawów aktywności i szablonów graficznych, aby utworzyć zadania dla uczniów w krótkim czasie. Kreator musi: o zawierać co najmniej dwa różne aktywności dwa szablony graficzne, w tym koniecznie sortowanie elementów i odwracane dwustronne karty z tekstem i/lub obrazem, o umożliwiać nauczycielom zapisanie treści danej aktywności ponownego jej użycia w innej aktywności, o pozwalać na wstawienie bezpośrednio do treści lekcji przygotowanych w kreatorze aktywności, bez konieczności opuszczania aplikacji do interaktywnych wyświetlaczy, o umożliwiać nauczycielom korzystanie z losowego wyboru ucznia na podstawie przygotowanej i zapisanej wcześniej listy uczniów danej klasy, o przygotowane ćwiczenia interaktywne mogą być rozwiązywane przez uczniów na interaktywnym wyświetlaczu lub poprzez sieć Internet na indywidualnych urządzeniach komputerowych każdego z uczniów. • Aplikacja do interaktywnych wyświetlaczy musi importować i eksportować pliki PowerPoint® oraz Interactive Whiteboard / Common File Format (IWB / CFF). • Oprogramowanie do interaktywnych wyświetlaczy musi pozwalać na wstawienie przez użytkowników tabel bezpośrednio do treści lekcji. Program pozwala przekształcić odręcznie narysowane tabele na tabele, które są już wstępnie sformatowane, na podstawie przekształcanego szkicu. • Aplikacja pozwala na grupowanie stron (treści pojedynczych tablic), tak aby możliwe było utworzenie korelacji z

		konspektami zajęć i harmonogramami oraz rozbicie materiału na segmenty w celu lepszej organizacji treści programowych. • Program musi zawierać kartę właściwości, która pozwala z jednego miejsca modyfikować style tekstu, animacje obiektów, efekty wypełnienia kształtów i style linii. • Musi zawierać narzędzie do graficznego odwzorowania pojęć (concept mapping). <u>Prowadzenie lekcji</u> • Program musi umożliwiać nauczycielowi prowadzenie i sterowanie treścią lekcji za pomocą tabletu działającego pod jednym z systemów operacyjnych Android lub iOS. • Aplikacja musi obsługiwać co najmniej dwie różne metody dotykowe, w celu uzyskania dostępu do menu wywoływanego kliknięciem prawym przyciskiem myszy, gdy program jest używany z kompatybilnym interaktywnym wyświetlaczem. • Oprogramowanie musi umożliwić użytkownikom wstawianie przeglądarek internetowych bezpośrednio do treści lekcji (wbudowana przeglądarka internetowa). Przeglądarka internetowa wyświetla „żywą", interaktywną zawartość internetową bezpośrednio na stronie. Użytkownicy muszą móc rysować i pisać po osadzonej zawartości strony internetowej oraz przeciągać i upuszczać obrazy z wbudowanej przeglądarki internetowej na stronę. • Program musi zawierać narzędzie do nagrywania i przechowywania aktywności na interaktywnym wyświetlaczu oraz dźwięku. Musi mieć możliwość nagrywania całego ekranu, okna lub określonego obszaru. Musi być w stanie dodać do nagrania znak wodny z znacznikiem czasu, informacją o dacie lub logo szkoły. • Musi umożliwić użytkownikom zresetowanie strony do ostatniego zapisanego stanu. • Musi umożliwić użytkownikom wyczyszczenie całego cyfrowego tuszu ze strony. • Musi zawierać narzędzie do pisania pozostawiające ślad, który zostaje wygładzony i wyrównany dla poprawy czytelności adnotacji. • Musi zawierać narzędzie do pisania, które pozwala na: o uruchamia efekt reflektora, po narysowaniu okręgu, o włącza lupę, po narysowaniu prostokąta, o pisane nim adnotacje blakną i znikają w ciągu kilku sekund. • Musi zawierać narzędzie umożliwiające użytkownikom wybranie do wyświetlania określonej części wstawionego do treści lekcji obrazu. • Musi zawierać opcję automatycznego wypełnienia dowolnego rysowanego ręcznie zamkniętego kształtu kolorem. • Musi zawierać narzędzie pisaka, który pozwala rysować kreską wyglądające jak ślad kredki świecowej w dowolnym kolorze. <u>Zawartość lekcji</u> • Aplikacja musi umożliwiać automatyczny i bezpośredni dostęp do lokalnego folderu sieciowego, w którym nauczyciele mogą przechowywać i modyfikować wspólną zawartość edukacyjną. • Oprogramowanie musi zapewniać dostęp do gotowych zasobów do nauki w społecznościowej witrynie internetowej bezpośrednio ze swojego interfejsu. • Dla użytkowników programu musi być zapewniony dostęp do co najmniej 500 lekcji. • Społecznościowa witryna internetowa dostawcy oprogramowania musi oferować on-line ponad 60 000 zasobów,

		w tym lekcje i aplikacje wydawnictw edukacyjnych oraz dostawców treści. Bezpłatne zasoby internetowe muszą być dostępne na żądanie i wyszukiwane według tematów oraz podkategorii. Użytkownicy muszą mieć możliwość podglądania zasobów przed pobraniem. Producent gwarantuje dostępność opisanych funkcji przez minimum rok od daty dostarczenia programu.

b) Projektor

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
1.	Technologia	3LCD
2.	Jasność	minimum 2700 ANSI lumenów w trybie pełnej jasności
3.	Kontrast	minimum 10000:1
4.	Rozdzielczość	minimum 1024x768, format matrycy 4:3 Projektor musi umożliwić wyświetlenie obrazu o przekątnej 80 cali (format 4:3) z odległości nie większej niż 65 cm (odległość od obrazu do najbardziej oddalonego od niej elementu projektora) przy zachowaniu proporcji obrazu, jego formatu, a także zapewniając ostrość na całej powierzchni bez stosowania jakichkolwiek elektronicznych korekcji
5.	Żywotność lampy	minimum 5000 godzin w trybie pełnej jasności
6.	Porty wejścia	a. 2 x VGA (DB-15), b. 2 x HDMI, c. 1 x composite video (RCA Chinch), d. 1 x audio stereo mini Jack e. 1 x audio stereo 2RCA f. 1 x RS232 g. 1 x RJ45 h. 1 x USB typ A i. 1 x USB typ B
7.	Porty wyjścia	j. 1 x VGA (DB-15), k. 1 x audio stereo mini Jack
8.	Waga	Max. 4,5kg
9.	Głośność pracy	(max) 34dB w trybie pełnej jasności
10.	Głośnik	Moc wbudowanych głośników minimum 15W
11.	Funkcjonalność	Zabezpieczenia antykradzieżowe kodem PIN; Filtr powietrza, który użytkownik sam może wymienić i wyczyścić bez konieczności demontażu projektora i użycia narzędzi; Wymiana lampy bez konieczności demontażu projektora; Funkcja blokady klawiatury uniemożliwiająca osobom niepowołanym na samodzielne włączenie i obsługę projektora bez nadzoru;
12.	Gwarancja	24 miesiące na lampę i projektor
13.	Regulacje	Minimalne płynne regulacje: wysokość góra/dół, odległość od ściany bliżej/dalej, pochylenie projektora przód/tył, pochylenie na prawo/lewo, odchylenie od ściany prawo/lewo Elektroniczna regulacja geometrii obrazu pozwalająca na regulację każdego narożnika i krawędzi obrazu z osobna
14.	Zabezpieczenie	Co najmniej 2 uchwyty do montażu mechanicznych zabezpieczeń przeciw kradzieżowych – przygotowane przez producenta projektora
15.	Uchwyt	Oryginalny uchwyt mocujący do ściany tego samego producenta co projektor

c) Montaż

Montaż	Wykonawca zobowiązany jest do montażu tablicy interaktywnej i projektora w miejscu wskazanym przez Zamawiającego.
	Montaż ścienny - Tablica interaktywna, projektor ultrakrótkoogniskowy w oparciu o dedykowany przez producenta uchwyt ścienny. Wyprowadzenie przewodów sygnałowych i zasilanie projektora. Kompletne przyłącze instalacyjne, wyposażone w puszkę natynkową, zawierające gniazda VGA, USB, Audio jack 3,5mm, okablowanie VGA, USB, Audio o długości min. 10m umożliwiające podłączenia projektora i tablicy do przyłącza. Instalacja oprogramowania do obsługi tablicy interaktywnej na sprzęcie dostępnym w danym pomieszczeniu montażu zestawu. Kalibracja sprzętu.
Szkolenie	Wykonawca zobowiązany jest do przeszkolenia wskazanych przez Zamawiającego pracowników (4 osoby) w zakresie działania, wykorzystania sprzętu.

5. Urządzenie Wielofunkcyjne – 1 szt.

Lp.	**Parametr**	**Wymagania minimalne**
1.	Funkcje	drukowanie, kopiowanie, skanowanie, faksowanie
2.	Prędkość druku	31 stron/minutę w czerni i w kolorze
3.	Technologia druku	Laser kolor
4.	Procesor	Min. 800MHz
5.	Pamięć wbudowana	512MB
6.	Podajnik papieru	Min. 250 arkuszy
7.	Podajnik dokumentów	Min. 50 arkuszy
8.	Podajnik uniwersalny	Min. 50 arkuszy
9.	Wyświetlacz	Kolorowy dotykowy o rozmiarze min. 9 cm
10.	Interfejsy	Gigabit Ethernet 10/100/1000, WiFi (IEEE 802.11b/g/n), USB
11.	Skanowanie	Dwustronne, do pliku (pdf, tiff, jpg, doc, xls, pdf z możliwością przeszukania), sieci, chmury, serwera email, USB
12.	Druk dwustronny	automatyczny
13.	Faks	Automatyczne faksowanie dwustronne,
14.	Gwarancja	3 lata
15.	Eksploatacja	Dołączone tonery o wydajności min. 3000 stron

6. Serwer + monitor LCD – 1sztuka

a) Serwer

Lp.	Parametry techniczne	Wymagane minimum
1	Obudowa	-obudowa typu Rack -wysokość nie więcej niż 1U -dostarczony wraz z szynami montażowymi do szafy rack umożliwiającymi pełne wysunięcie z szafy, uchylnym ramieniem dla prowadzenia kabli podczas wysuwania i wsuwania serwera w szafie rack

Lp.	Parametry techniczne	Wymagane minimum
2	Procesor	-zainstalowany procesor osiągający w testach wydajności SPECint_rate2006 min. 215 pkt. -do oferty należy dołączyć pełen protokół testów SPEC dla oferowanego modelu serwera wraz z oferowanym CPU -maksymalny pobór mocy dla procesora max 73 Watt.
3	Płyta główna	-dedykowana serwerowa, -minimum 3 sloty PCI Express w tym minimum 2 sloty generacji 3 o prędkości x8; -minimum 4 gniazda pamięci RAM DDR4
4	Pamięć RAM	-nie mniej niż 32GB RAM DDR4-2400MHz w dwóch kościach po 16GB każda, pozostawione 2 wolne sloty pamięci do dalszej rozbudowy -zabezpieczenie pamięci mechanizmem ECC -możliwość rozbudowy do minimum 64 GB RAM
5	HDD	-dyski hotplug -możliwość instalacji 4 dysków 3,5” hotplug; -Fabrycznie zainstalowane dwa dyski twarde typu hotplug 3,5” 2TB SATA 7200 RPM
6	Kontroler dysków	Kontroler RAID SATA 0/1/10
7	Napęd optyczny	DVD +/- RW wewnętrzny
8	Karta graficzna	Zintegrowana z płytą główną , minimum 32MB pamięci RAM, wsparcie dla rozdzielczości minimum 1280x1024;
9	Karty sieciowe	-2x LAN 1Gbit/s ze wsparciem iSCSI, RJ-45; -zintegrowana, dedykowana karta LAN 1Gbit/s do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym serwera
10	Zasilanie i chłodzenie	-dwa, nadmiarowe zasilacze hotplug o mocy maksymalnej nie więcej niż 460W, o maksymalnej sprawności minimum 94% (potwierdzenie na podstawie dokumentacji technicznej producenta serwera) - możliwość zamontowania w miejscu drugiego zasilacza modułu bateryjnego o mocy min. 360W -nadmiarowy układ chłodzenia (redundancja typu N+1)
11	Zarządzanie zdalne, inwentaryzacja	-Umieszczona z przodu chowana karta identyfikacyjna serwera zawierająca nazwę serwera, numer handlowy, numer seryjny, adresy MAC kart sieciowych -Zintegrowany trwale z płytą główną kontroler zdalnego zarządzania zgodny ze standardem IPMI 2.0 umożliwiający: • zdalne uruchomienie, wyłączenie i restart serwera, pełne

Lp.	Parametry techniczne	Wymagane minimum
		zarządzanie sprzętowe: monitorowanie pracy kluczowych układów, wentylatorów, zasilaczy, napędów, temperatur, itp., logowanie błędów w zakresie ustalonym przez administratora • dostęp do interfejsu karty zarządzającej za pomocą przeglądarki MS Internet Explorer lub Mozilla Firefox bez konieczności instalowania jakiegokolwiek software specyficznego dla producenta sprzętu • Opcjonalne przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów (CD, DVD, FDD, klucz USB) i ich obrazów na poziomie sprzętowym (cyfrowy KVM) • połączenie z kartą zarządzającą musi być szyfrowane minimum 128 bitowym kluczem SSL • monitorowanie zużycia energii serwera w trybie rzeczywistym i wizualizacja raportów w postaci wykresów graficznych, • dedykowana karta LAN 1 Gb/s do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym serwera. • możliwość konfiguracji 16 niezależnych kont administracyjnych (dostępowych) do karty zarządzającej, logowanie aktywności użytkowników, wsparcie dla integracji z Active Directory i LDAP • wsparcie dla aktualizacji firmware karty zarzadzającej online, bez konieczności restartu serwera
12	Porty	-Minimum 6 portów USB 3.0 w tym 2 porty USB z przodu obudowy, minimum 4 porty w standardzie USB 3.0 z tyłu - 1x VGA (15-stykowe) -port szeregowy, minimum dwa porty RJ45 -nie dopuszcza się stosowania przejściówek, adapterów oraz rozgałęziaczy i przedłużaczy.
13	Oprogramowanie	Dostarczone wraz z serwerem oprogramowanie zarządzające i diagnostyczne wyprodukowane i wspierane przez producenta serwera umożliwiające m.in.: • konfigurację kontrolera RAID bez konieczności konfiguracji bezpośrednio w BIOS kontrolera • instalację systemów operacyjnych wspieranych przez producenta serwera (z nośników fizycznych lub zdalnie przez sieć LAN) wraz ze sterownikami • tworzenie i zapis plików konfiguracyjnych umożliwiających zwielokrotnioną, automatyczną instalację systemu i konfigurację serwera • zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanej karty zarządzającej oraz informacji z systemu operacyjnego, przekierowanie informacji i alertów poprzez email, bramkę SMS, popup. • monitorowanie i zarządzanie kontrolerami RAID i zainstalowanymi dyskami twardymi
14	Wsparcie dla systemów operacyjnych	Wymagana kompatybilność i wsparcie serwera dla następujących systemów operacyjnych: Microsoft Windows 2016,
15	Certyfikaty producenta	Certyfikat producenta ISO 9001 w zakresie projektowania, produkcji i

Lp.	Parametry techniczne	Wymagane minimum
		serwisu produktów, CE oraz ISO 14001.
16	Okablowanie	Dołączone kable zasilające
17	Gwarancja	5 lat gwarancji producenta, w miejscu instalacji, czas reakcji serwisu – następny dzień roboczy -dostępność części zamiennych co najmniej 5 lat po zakończeniu produkcji serwera (potwierdzone przez producenta)
18	Inne	-Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane (wymagane oświadczenie producenta dołączone do oferty) oraz muszą być objęte gwarancją producenta, potwierdzoną przez oryginalne karty gwarancyjne; -Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce - Wymagane oświadczenie producenta serwera, że oferowany do przetargu sprzęt spełnia ten wymóg; -Oferent zobowiązany jest dostarczyć wraz z ofertą kartę produktową oferowanego serwera umożliwiającą weryfikację parametrów oferowanego sprzętu; -Ogólnopolska, telefoniczna infolinia/linia techniczna producenta komputera, (ogólnopolski numer o zredukowanej odpłatności 0-800/0-801, w ofercie należy podać nr telefonu) w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; -Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;

b) Monitor

Lp.	**Parametr**	**Wymagania minimalne**
1.	Przekątna ekranu	21,5”; 54,7cm
2.	Format obrazu	16:9
3.	Rozdzielczość fizyczna	Full HD, 1920x1080 pikseli @75Hz (2.1 megapixela)
4.	Jasność	250 cd/m^2
5.	Kontrast	3000:1
6.	Kontrast dynamiczny	80 000 000:1 ACR
7.	Czas reakcji matrycy	4 ms
8.	Kąty widzenia	Poziomo/pionowo: 178/178 stopni, prawo/lewo: 89/89 stopni, góra/dół 89/89 stopni
9.	Wyświetlane kolory	16,7 mln
10.	Redukcja niebieskiego światła	Tak
11.	Plamka matrycy	0,248 mm
12.	Częstotliwość pozioma	30-80 kHz
13.	Częstotliwość pionowa	55-75 Hz
14.	Wejścia sygnałowe	1x D-Sub (VGA), 1x HDMI, 1x DisplayPort
15.	Głośniki	Wbudowane 2x1W, dodatkowe wyjście słuchawkowe
16.	Kąty pochylenia	22 stopnie w górę, 5 stopni w dół
17.	Standard VESA	100x100
18.	Zasilacz	Wewnętrzny, AC 100-240V, 50/60Hz
19.	Zużycie energii	Typowa 21W

20.	Dołączone akcesoria	Kabel zasilający, kabel HDMI, kabel DisplayPort
21.	Gwarancja producenta	3 lata na monitor, 30 dni gwarancja producenta 0 pixeli/subpixeli
22.	Certyfikaty	CE, ISO 9001 i 14001 dla producenta, TCO 6.0 lub równoważny

7. Switch 24-portowy zarządzany – 1szt.

Lp.	Nazwa komponentu	Wymagania minimalne
1.	Architektura sieci LAN	GigabitEthernet
2.	SmartSwitch (WEB Managed)	Tak
3.	Liczba portów 1000BaseT (RJ45)	24 szt.
4.	Liczba gniazd MiniGBIC (SFP)	2 szt.
5.	Porty komunikacji	• 10/100/1000 Base-T (RJ45) • 100/1000X Fiber SFP
6.	Zarządzanie, monitorowanie i konfiguracja	• zarządzanie przez przeglądarkę WWW • DHCP Client - Dynamic Host Configuration Protocol
7.	Protokoły uwierzytelniania i kontroli dostępu	• IEEE 802.1x - Network Login • ACL bazujący na adresach MAC • ACL bazujący na adresach IP i typie protokołu
8.	Obsługiwane protokoły routingu	ruting statyczny
9.	Obsługiwane protokoły i standardy	• IEEE 802.3z - 1000BaseSX/LX • IEEE 802.3ae - 10-GigabitEthernet • IEEE 802.3ad - Link Aggregation Control Protocol • IEEE 802.1AB - Link Layer Discovery Protocol • IEEE 802.1p - Priority • IEEE 802.1Q - Virtual LANs • IEEE 802.3i 10BASE-T Ethernet • IEEE 802.3u - 100BaseTX • IEEE 802.3ab - 1000BaseT • IEEE 802.3x - Flow Control • IEEE 802.1D - Spanning Tree • IEEE 802.1s - Multiple Spanning Tree • IEEE 802.1w - Rapid Convergence Spanning Tree • IEEE 802.1x - Network Login • IEEE 802.1AB - Link Layer Discovery Protocol • IGMP - Internet Group Management Protocol • ToS - Type of service • QoS - Quality of Service (kontrola jakość usług i przepustowości) • DHCP - Dynamic Host Configuration Protocol • ACL - Access Control List
10.	Rozmiar tablicy adresów MAC	16000
11.	Prędkość magistrali wew.	52 Gb/s
12.	Bufor pamięci	2 MB
13.	Warstwa przełączania	2
14.	Typ obudowy	1U Rack
15.	Maksymalny pobór mocy	17 Wat
16.	Wyposażenie standardowe	• przewód zasilający • zestaw do montażu w szafie rack 19" • oprogramowanie na CD

17.	Dodatkowe funkcje	• Ochrona hasłem • port mirroring - przekierowanie informacji o ruchu na wskazany port • zabezpieczenie przed atakami typu DoS (Denial of Service)
18.	Gwarancja	• min. 36 miesięcy

8. Zasilacz awaryjny UPS – 1 szt.

Lp.	Nazwa komponentu	Wymagania minimalne
1	Moc pozorna	Min. 1500 VA
2	Moc rzeczywista	Min. 1350 Wat
3	Architektura UPSa	line-interactive
4	Maks. czas przełączenia na baterię	10 ms
5	Liczba i rodzaj gniazdek z utrzymaniem zasilania	8 x IEC320 C13 (10A)
6	Typ gniazda wejściowego	IEC320 C14 (10A)
7	Czas podtrzymania dla obciążenia 100%	Min. 3 min
8	Czas podtrzymania przy obciążeniu 50%	Min. 9 min
9	Zakres napięcia wejściowego w trybie podstawowym	220-240 V
10	Zmienny zakres napięcia wejściowego	0-300 V
11	Zimny start	Tak
12	Układ automatycznej regulacji napięcia (AVR)	Tak
13	Sinus podczas pracy na baterii	Tak
14	Porty komunikacji	• USB • RS232 (DB9) • SmartSlot
15	Port zabezpieczający linie danych	RJ45 - linia modemowa/faxowa, DSL, 10/100BaseTX
16	Diody sygnalizacyjne	Wyświetlacz LCD
17	Alarmy dźwiękowe	• praca z baterii • awaria sieci zasilającej • znaczne wyczerpanie baterii
18	Typ obudowy	• 2U Rack
19	Wyposażenie standardowe	• Instrukcja obsługi • Kabel zasilający • Kabel USB • oprogramowanie na CD • 2 x kabel wyjściowy IEC • kabel szeregowy RS232 (DB9)
20	Dołączone oprogramowanie	- Możliwość kontrolowania i monitorowania wielu jednostek UPS z sieci lokalnej i Internetu - Wykresy analizy mocy, statystyki zdarzeń, eksport historii danych - Wykres danych jednostki UPS w czasie rzeczywistym (napięcie, częstotliwość, poziom obciążenia, poziom naładowania baterii)

		- Bezpieczne wyłączenie systemu i ochrona danych przed awarią zasilania - Powiadomienia za pomocą dźwięków systemowych, e-mail, SMS, do wszystkich komputerów w sieci LAN - Harmonogram włączenia/wyłączenia, test baterii, programowana kontrola gniazda, kontrola alarmów dźwiękowych. - Ochrona dostępu hasłem, dostęp zdalny i zarządzanie
21	Akcesoria	• Zestaw szyn montażowych do szaf 19"
22	Dodatkowe informacje	• Czas ładowania baterii 4h - 90% • Automatyczny restart po powrocie zasilania

9. Szafa teleinformatyczna – 1 szt.

Lp.	Nazwa komponentu	Wymagania minimalne
1	Wysokość wewnętrzna	42 U
2	Wysokość	2055 mm
3	Szerokość	600 mm
4	Głębokość	1000 mm
5	Maksymalna nośność	800 kg
6	Dodatkowe informacje	• Drzwi przednie przeszklone z zamkiem • Drzwi tylne stalowe uchylne z zamkiem • Drzwi boczne demontowane na zatrzaskach z możliwością montażu zamka • Wyposażenie: 4 wentylatory, 3 półki, listwa zasilająca, 40 koszyków ze śrubami • Zgodne z standardami ANSI / EIA RS-310-D, DIN 41491 • Zgodność z normami PART1, IEC297-2, DIN41494 • Zgodność z normami PART7, GB/T3047.2-92 • Kompatybilne ze standardami: metrycznym, ETSI oraz międzynarodowym 19” • Szkielet o nośności do 800kg • Stalowa blacha zimnowalcowana • Wykończenie pow.: odtłuszczanie, wytrawianie, fosfatowanie, malowanie proszkowe • Zabezpieczona przed rdzą, utlenianiem, porysowaniem, korozją • Dwa przepusty kablowe - szczotkowy w suficie , kablowy w podłodze • Grubość ramy: 1.5 mm • Grubość szyn montażowych: 2.0 mm • Grubość paneli bocznych: 1.2 mm • Grubość szkła: 5 mm • Regulowane nóżki i kółka o dużej wytrzymałości • Kolor - RAL9004 • Stopień ochrony: IP20 • Kompatybilność ze sprzętem różnych producentów
7	Kolor	Czarny

10. Oprogramowanie antywirusowe z firewall – subskrypcja na 36 miesięcy, licencja dla stacji roboczych i serwerów (19 licencji)

1. Pełne wsparcie dla systemu Windows XP SP3/Vista/Windows 7/Windows8/Windows 8.1/Windows 8.1 Update/10

2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows.
3. Wersja programu dla stacji roboczych Windows dostępna zarówno w języku polskim jak i angielskim.
4. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim.
5. Skuteczność programu potwierdzona nagrodami VB100 i AV-comparatives

Ochrona antywirusowa i antyspyware

6. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
7. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
8. Wbudowana technologia do ochrony przed rootkitami.
9. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
10. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
11. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
12. System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania.
13. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
14. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
15. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
16. Możliwość skanowania dysków sieciowych i dysków przenośnych.
17. Skanowanie plików spakowanych i skompresowanych.
18. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
19. Wykluczenie ze skanowania musi odbywać się nie tylko po nazwie pliku ale również ma być możliwe użycie symbolu wieloznacznego „*” zastępującego dowolne znaki w ścieżce.
20. Administrator ma możliwość dodania wykluczenia po tzw. HASH’u zagrożenia, wskazującego bezpośrednio na określoną infekcję a nie konkretny plik.
21. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
22. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
23. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.
24. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
25. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
26. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
27. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego).

28. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
29. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
30. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
31. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
32. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
33. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony.
34. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora.
35. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
36. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
37. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
38. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta.
39. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
40. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
41. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.
42. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
43. W przypadku gdy stacja robocza nie będzie posiadała dostępu do sieci Internet ma odbywać się skanowanie wszystkich procesów również tych, które wcześniej zostały uznane za bezpieczne.
44. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
45. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń mają być wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
46. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.

47. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
48. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
49. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
50. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.
51. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.
52. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
53. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji.
54. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
55. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.
56. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
57. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
58. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM , urządzeń przenośnych oraz urządzeń dowolnego typu.
59. Funkcja blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model.
60. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia, dana funkcjonalność musi pozwalać na automatyczne wypełnienie właściwości urządzenia dla tworzonej reguły.
61. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie brak dostępu do podłączanego urządzenia.
62. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
63. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
64. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika
65. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).

66. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    - tryb automatyczny z regułami gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    - tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    - tryb oparty na regułach gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    - tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach.
    - Tryb inteligentny – w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.
67. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
68. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
69. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
70. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp.
71. Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.
72. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.
73. Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
74. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
75. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.
76. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur.
77. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.
78. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http
79. Program musi być wyposażony w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback).
80. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).
81. Program ma być w pełni zgodny z technologią CISCO Network Access Control.
82. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym.
83. W momencie wykrycia trybu pełno ekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji.

84. Użytkownik ma mieć możliwość skonfigurowania programu tak aby automatycznie program włączał powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym po określonym przez użytkownika czasie.
85. Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania.
86. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
87. Program musi posiadać możliwość utworzenia z poziomu interfejsu aplikacji dziennika diagnostycznego na potrzeby pomocy technicznej.
88. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline.
89. Możliwość podejrzenia licencji za pomocą, której program został aktywowany.
90. W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: ochrona antywirusowa i antyspyware, kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, , Obsługa technologii Microsoft NAP.
91. W programie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji.
92. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej.
93. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas po którym automatycznie zostają przywrócone dotychczasowe ustawienia.
94. Administrator ma możliwość wstrzymania polityk na 10 min, 30 min, 1 godzinę i 4 godziny
95. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika.
96. Program musi posiadać opcję automatycznego skanowania komputera po dokonaniu zmian z użyciem opcji wstrzymania polityki.
97. Aplikacja musi posiadać funkcję ręcznej aktualizacji komponentów programu.
98. Możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych.
99. Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi np. powiadomień o wyłączonych mechanizmach ochrony czy stanie licencji.
100. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.

Ochrona przed spamem

101. Ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.
102. Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.
103. Pełna integracja z programami pocztowymi MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail – antyspamowe funkcje programu dostępne są bezpośrednio z paska menu programu pocztowego.
104. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.

105. Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną wiadomość i odwrotnie oraz ręcznego dodania wiadomości do białej i czarnej listy z wykorzystaniem funkcji programu zintegrowanych z programem pocztowym.
106. Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam.
107. Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam.
108. Program ma umożliwiać współpracę w swojej domyślnej konfiguracji z folderem „Wiadomości śmieci" obecnym w programie Microsoft Outlook.
109. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną zmieni jej właściwość jako „nieprzeczytana" oraz w momencie zaklasyfikowania wiadomości jako spam na automatyczne ustawienie jej właściwości jako „przeczytana".
110. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

Zapora osobista (personal firewall)

111. Zapora osobista ma pracować jednym z 4 trybów:
    - tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące, jednocześnie umożliwia utworzenie dodatkowych reguł przez administratora
    - tryb interaktywny – program pyta się o każde nowe nawiązywane połączenie i automatycznie tworzy dla niego regułę (na stałe lub tymczasowo),
    - tryb oparty na regułach – użytkownik/administrator musi ręcznie zdefiniować reguły określające jaki ruch jest blokowany a jaki przepuszczany,
    - tryb uczenia się – umożliwia zdefiniowanie przez administratora określonego okresu czasu w którym oprogramowanie samo tworzy odpowiednie reguły zapory analizując aktywność sieciową danej stacji.
112. Program musi akceptować istniejące reguły w zaporze systemu Windows, zezwalające na ruch przychodzący.
113. Możliwość tworzenia list sieci zaufanych
114. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie
115. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.
116. Możliwość wyboru jednej z 3 akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj o decyzję.
117. Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń.
118. Możliwość zapisywania w dzienniku zdarzeń związanych z zezwoleniem lub zablokowaniem danego typu ruchu.
119. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet.
120. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
121. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet.
122. Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu.
123. Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.
124. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
125. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci
126. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.
127. Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera

DHCP, lokalny adres IP, identyfikator SSID, szyfrowaniu sieci bezprzewodowej lub jego braku, aktywności połączenia bezprzewodowego lub jego braku, konkretny interfejs sieciowy w systemie.

128. Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS zarówno z wykorzystaniem adresów IPv4 jak i IPv6
129. Opcje związane z autoryzacją stref mają oferować opcje łączenia (np. lokalny adres IP i adres serwera DNS) w dowolnej kombinacji celem zwiększenia dokładności identyfikacji danej sieci.
130. Program musi możliwość ustalenia tymczasowej czarnej listy adresów IP, które będą blokowane podczas próby połączenia.
131. Program musi posiadać kreator, który umożliwia rozwiązać problemy z połączeniem. Musi on działać w oparciu o:
    - rozwiązanie problemów z aplikacją lokalną którą wskazujemy z listy.
    - rozwiązywanie problemów z połączeniem z urządzeniem zdalnym na podstawie adresu IP.

Kontrola dostępu do stron internetowych

132. Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych.
133. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły.
134. Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego.
135. Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.
136. Aplikacja musi posiadać możliwość filtrowania url w oparciu o co najmniej 140 kategorii i pod kategorii.
137. Podstawowe kategorie w jakie aplikacja musi być wyposażony to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii.
138. Moduł musi posiadać także możliwość grupowania kategorii już istniejących.
139. Lista adresów url znajdujących się w poszczególnych kategoriach musi być na bieżąco aktualizowana przez producenta.
140. Użytkownik musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych.
141. Aplikacja musi posiadać możliwość określenia uprawnień dla dostępu do kategorii url – zezwól, zezwól i ostrzeż, blokuj.
142. Program musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania określonej w regułach witryny.

Ochrona serwera plików Windows

1. Wsparcie dla systemów: Microsoft Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2, 2016, SBS 2003, SBS 2003 R2, SBS 2008, SBS 2011, Microsoft MultiPoint Server 2010, Microsoft MultiPoint Server 2011, Windows MultiPoint Server 2012.
2. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
4. Wbudowana technologia do ochrony przed rootkitami i exploitami.
5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
7. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
8. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
9. System antywirusowy ma mieć możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
10. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.
11. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego.
12. Możliwość skanowania dysków sieciowych i dysków przenośnych.
13. Skanowanie plików spakowanych i skompresowanych.
14. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
15. Program musi posiadać funkcjonalność pozwalającą na ograniczenie wielokrotnego skanowania plików w środowisku wirtualnym za pomocą mechanizmu przechowującego informacje o przeskanowanym już obiekcie i współdzieleniu tych informacji z innymi maszynami wirtualnymi.
16. Aplikacja powinna wspierać mechanizm klastrowania.
17. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
18. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS.
19. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
20. Program ma umożliwiać użytkownikowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, płyt CD/DVD i pamięci masowych FireWire.
21. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia.
22. Aplikacja musi posiadać funkcjonalność, która automatycznie uzupełni elementy wymagane dla tworzenia reguł w oparciu o informacje dostępne z aktualnie podłączonego nośnika.
23. Aplikacja ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, brak dostępu do podłączanego urządzenia.
24. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
25. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
26. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
27. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
28. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.
29. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
30. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.
31. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione.
32. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.
33. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).

34. Możliwość przeniesienia zainfekowanych plików w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
35. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
36. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.
37. Aktualizacje modułów analizy heurystycznej.
38. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
39. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
40. Wysyłanie zagrożeń do laboratorium ma być możliwe z serwera zdalnego zarządzania i lokalnie z każdej stacji roboczej w przypadku komputerów mobilnych.
41. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
42. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
43. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.
44. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła.
45. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło.
46. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo.
47. System antywirusowy ma być w pełni zgodny z technologią CISCO NAC.
48. System antywirusowy ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.
49. System antywirusowy ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Program ma także posiadać opcję dezaktywacji tego mechanizmu.
50. Po instalacji systemu antywirusowego, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.
51. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
52. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
53. Program powinien umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: nośników CD/DVD oraz urządzeń USB.
54. System antywirusowy ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych

aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.
55. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.
56. System antywirusowy ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
57. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
58. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).
59. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
60. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja).
61. Do każdego zadania aktualizacji można przypisać dwa różne profile z innym ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja). Przykładowo, domyślny profil aktualizuje z sieci lokalnej a w przypadku jego niedostępności wybierany jest profil rezerwowy pobierający aktualizację z Internetu.
62. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
63. Aplikacja musi wspierać skanowanie magazynu Hyper-V
64. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów
65. Wykluczenie ze skanowania musi odbywać się nie tylko po nazwie procesu ale również ma umożliwiać użycie symbolu wieloznacznego „*” zastępującego inne znaki.
66. Administrator ma możliwość dodania wykluczenia po tzw. HASH’u zagrożenia, wskazującego bezpośrednio na określoną infekcję a nie konkretny plik.
67. Praca programu musi być niezauważalna dla użytkownika.
68. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania.
69. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

Administracja zdalna

1. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2003, 2008, 2012 oraz systemach Linux.
2. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance).
3. Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL.
4. Serwer administracyjny musi oferować możliwość wykorzystania już istniejącej bazy danych MS SQL lub MySQL użytkownika.
5. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów oddzielnie bezpośrednio ze strony producenta.
6. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej.
7. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy występujące w sieci.
8. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6.
9. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający.

10. Zmiana języka panelu administracyjnego nie może wymagać zatrzymania lub reinstalacji oprogramowania zarządzającego.
11. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL.
12. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
13. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
14. Jeden centralny serwer centralnego zarządzania bez względu na wielkość sieci.
15. Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci –serwer pośredniczący (proxy) lub serwer centralny.
16. Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym.
17. Serwer proxy musi być wyposażony we własną bazę danych, w której będą przechowywane dane z agentów na wypadek braku połączenia z serwerem centralnym.
18. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.
19. Serwer administracyjny musi oferować możliwość instalacji serwera http proxy pozwalającego na pobieranie aktualizacji baz sygnatur oraz pakietów instalacyjnych na stacjach roboczych bez dostępu do Internetu.
20. Serwer http proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) najczęściej pobieranych elementów.
21. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
22. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.
23. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na stacjach roboczych z systemami Windows, Mac OS X oraz Linux oraz serwerach Windows.
24. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na urządzeniach mobilnych z systemem Android.
25. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.
26. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
27. Administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami nie posiadającymi zainstalowanego programu zabezpieczającego.
28. Agent musi przekazywać informacje na temat stanu systemu operacyjnego do serwera administracji zdalnej.
29. Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania.
30. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
31. Instalacja agenta musi odbywać się przy wykorzystaniu repozytorium producenta. Repozytorium powinno zawierać aktualne wersje agentów bez względu na rodzaj systemu operacyjnego.
32. Instalacja agenta nie może wymagać określenia typu systemu (32 lub 64 – bitowy) oraz jego rodzaju (Windows, Mac, itp) a dobór odpowiedniego pakietu musi być w pełni automatyczny.
33. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika.
34. W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play.
35. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.

36. Serwer administracyjny musi oferować możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, nie komunikację za pośrednictwem wiadomości SMS.
37. Serwer administracyjny musi oferować możliwość utworzenia polityk konfiguracji dla aplikacji zabezpieczającej na urządzeniu mobilnym.
38. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi.
39. Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej
40. Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji.
41. Administrator musi posiadać możliwość utworzenia użytkownika wbudowanego lub zintegrowanego z grupą z usługi Active Directory.
42. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp.
43. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis.
44. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
45. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta bez konieczności logowania się do panelu administracyjnego.
46. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany.
47. Dostępne zadania muszą być podzielone na dwie grupy: zadania klienta oraz zadania serwera.
48. Zadania serwera obejmujące zadanie instalacji agenta, generowania raportów oraz synchronizacji grup.
49. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.
50. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.
51. Serwer administracyjny musi w przejrzysty sposób informować administratora o elementach zadań jakie są wymagane do jego uruchomienia a w przypadku jego braku wskazywać brakujące elementy konfiguracji.
52. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym.
53. Serwer administracyjny musi oferować możliwość wyboru parametrów pakietu instalacyjnego zależnych od systemu operacyjnego oraz licencji na program zabezpieczający.
54. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu.
55. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką.
56. Serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy.
57. Serwer administracyjny musi oferować możliwość uruchomienia zadania automatycznie zgodnie z harmonogramem, po wystąpieniu nowego dziennika zdarzeń lub umieszczeniu nowego klienta w grupie dynamicznej.
58. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów.
59. Grupy dynamiczne tworzone na podstawie szablonu określającego warunki jakie musi spełnić klient aby zostać umieszczony w danej grupie. Przykładowe warunki: Adresy sieciowe IP, Aktywne zagrożenia, Stan funkcjonowania/ochrony, Wersja systemu operacyjnego, itp.

60. Serwer administracyjny musi oferować możliwość utworzenia polityk dla programów zabezpieczających i modułów serwera centralnego zarządzania.
61. Serwer administracyjny musi oferować możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. Serwer administracyjny musi oferować możliwość przypisania kilku polityk z innymi priorytetami dla jednego klienta.
62. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej.
63. Serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś" dla konkretnej opcji w konfiguracji klienta. Opcja ta nie będzie mogła być zmieniona na stacji klienckiej bez względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku.
64. Serwer administracyjny musi oferować możliwość ukrycia graficznego interfejsu użytkownika na stacji klienckiej i jego uruchomienia tylko przez administratora.
65. Serwer administracyjny musi umożliwiać wyświetlenie polityk do których przynależy dana stacja robocza oraz ich edycję z poziomu właściwości samego klienta
66. Serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów.
67. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania.
68. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie.
69. Serwer administracyjny musi oferować możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy, itp.
70. Serwer administracyjny musi oferować możliwość określenia danych jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na elementach wykresu oraz ich odfiltrowania i posortowania.
71. Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów.
72. Serwer administracyjny powinien posiadać Panel kontrolny z raportami administratora, pozwalający na szybki dostępu do najbardziej interesujących go danych. Panel ten musi oferować możliwość modyfikacji jego elementów.
73. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW.
74. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS.
75. Serwer administracyjny musi oferować możliwość skonfigurowania czasu automatycznego odświeżania raportu na panelu kontrolnym oraz umożliwiać jego odświeżenie na żądanie.
76. Serwer administracyjny musi oferować możliwość tworzenia wielu zakładek panelu, w których będą widoczne wybrane przez administratora elementy monitorujące.
77. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego.
78. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
79. Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień lub skorzystanie z predefiniowanych wzorów.
80. Powiadomienia muszą dotyczyć zmiany ilości klientów danej grupy dynamicznej, wzrostu liczby grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń lub skanowania lub stanu obiektu serwer centralnego zarządzania.
81. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP.
82. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu.
83. Serwer administracyjny musi oferować możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.

84. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta.
85. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji.
86. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty.
87. Serwer administracyjny musi oferować możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.
88. Narzędzie administracyjne musi być wyposażone w mechanizm wyszukiwania zarządzanych komputerów na podstawie co najmniej nazwy komputera, adresu IPv4 i IPv6 lub wyszukania konkretnej nazwy zagrożenia.
89. Serwer administracyjny musi być wyposażony w machizm autodopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana.
90. Serwer administracji musi umożliwić granulację uprawnień dla Administratorów w taki sposób, aby każdemu z nich możliwe było przyznanie oddzielnych uprawnień do poszczególnych grup komputerów, polityk lub zadań.
91. Konfiguracja zestawów uprawnień musi umożliwiać przypisanie praw tylko do odczytu, odczytu i użycia, oraz prawo do zapisania zmian w ramach danego zadania lub polityki w konsoli ERA.
92. Konsola webowa musi umożliwiać stronicowanie w widoku komputerów w celu ograniczenia liczby wyświetlanych maszyn na jednej stronie.
93. Administrator musi mieć możliwość podłączenia do stacji roboczej z użyciem protokołu RDP bezpośrednio z poziomu konsoli ERA.
94. Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar
95. Musi istnieć mechanizm, umożliwiający dodawanie reguł do istniejących już w module firewalla lub harmonogramie. Takie reguły można umieścić na początku lub końcu istniejącej listy.
96. Konsola administracyjna musi umożliwiać dodanie własnego logotypu do interfejsu webowego.

11. Oprogramowanie do zarządzania pracownią komputerową – 1 licencja

a) System operacyjny do serwera

Wymagana licencja na 16 rdzeni wraz z licencjami dostępowymi do serwera dla 18 użytkowników.

Licencje na serwerowy system operacyjny muszą być przypisane do każdego rdzenia procesora fizycznego na serwerze. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowisk serwerowego systemu operacyjnego niezależnie od liczby rdzeni w serwerze fizycznym.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.

6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
    a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
    b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
    c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
    d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18. Mechanizmy logowania w oparciu o:
    a. Login i hasło,
    b. Karty z certyfikatami (smartcard),
    c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..
20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,

b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
    i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
    ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
    iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
    iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
c. Zdalna dystrybucja oprogramowania na stacje robocze.
d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
    i. Dystrybucję certyfikatów poprzez http
    ii. Konsolidację CA dla wielu lasów domeny,
    iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
    iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
f. Szyfrowanie plików i folderów.
g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
i. Serwis udostępniania stron WWW.
j. Wsparcie dla protokołu IP w wersji 6 (IPv6),
k. Wsparcie dla algorytmów Suite B (RFC 4869),
l. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
m. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
    i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
    ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
    iii. Obsługi 4-KB sektorów dysków
    iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
    v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
    vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.

27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
31. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

b) Licencja na oprogramowanie sieciowe chroniące uczniów/studentów przed niepożądanymi treściami/stronami z Internetu na 18 stanowisk z możliwością:

- obejrzenia historii odwiedzanych stron na dowolnej stacji roboczej,

- całkowitej blokady dostępu do Internetu

- podejrzenia ekranu dowolnej stacji roboczej- tzw. zdany pulpit,

- zdalnej instalacji programu

12. Sieć komputerowa

1. **Wykonanie tras kablowych.**

Wykonanie instalacji sieciowej.

Trasy kablowe w pomieszczeniu dla punktów PEL1 (Punkt Elektryczno-Logiczny) należy ułożyć w podłodze z zachowaniem standardów bezpieczeństwa. Montaż osprzętu elektryczno logicznego na zasadzie podłogowej (puszki podłogowe zamykane) z możliwością szybkiego zabezpieczenia po wypięciu wtyczek tj. metalowa podstawa puszki wraz z zaślepką na czas prac budowlanych.

Trasy kablowe w pomieszczeniu dla punktów PEL2 należy ułożyć w podłodze z zachowaniem standardów bezpieczeństwa, zamawiający dopuszcza montaż osprzętu elektryczno logicznego w standardzie 45x45mm na bazie kanału kablowego.

Dla całości tras kablowych Zamawiający wymaga zachowania ciągłości trasy na każdym odcinku oraz stosowania gotowych elementów wykańczających(przedłużenia, zakręty, kąty, zaślepki) dedykowanych do systemu zastosowanego przez Wykonawcę. Trasy kablowe należy wykonać zgodnie z rys nr 1 stanowiącym załącznik do OPZ.

2. **Wykonanie PEL.**

Zamawiający określa jako PEL kompletny zamocowany zestaw 2 gniazd elektrycznych 230V i 2 gniazd RJ45 kat. 6 całość w standardzie 45x45mm. Trwale i estetycznie zamontowanych. Gniazda logiczne opisane zgodnie ze wskazaniem Zamawiającego.

Ilość PEL określa się na 27 szt. Rozmieszczenie PEL 1 oraz PEL 2 zostało przedstawione na rysunku dołączonym do zapytania.

3. **Punkty dystrybucyjne1 logiczne i elektryczne.**

Zamawiający określa jako punkty dystrybucyjne logiczne panele krosowe kategorii 6 wypełnione modułami RJ45 typu keystone kategorii 6 zamontowane w szafie dystrybucyjnej typu RACK.

Zamawiający określa jako punkty dystrybucyjne elektryczne rozdzielnię elektryczną wyposażoną

zgodnie z obowiązującymi normami, z której są zasilane PEL w części elektrycznej, przy zachowaniu standardu ,max 3 PEL na jednym obwodzie elektrycznym z zabezpieczeniem różnicowo-prądowym.

Kable sieciowe UTP kat 5E/6 w formie linki.

Kabek zasilający YDY 3 x 2,5 poprowadzony w rurkach plastikowych karbowanych giętkich (peszel). Zamawiający wymaga pomiarów elektrycznych, podpisanych i opieczętowanych przez osobę posiadającą uprawnienia.

Zamawiający wymaga aby pomiary logiczne wykonano testerem FLUKE DTX-1800 lub równoważnym.
Na zakończenie prac zamawiający wymaga załączyć dokładny test z w/w urządzenia do dokumentacji powykonawczej.

Po wykonaniu instalacji sieciowo elektrycznej Wykonawca udostępni pomieszczenie firmie, która wykona wyrównania podłogi oraz położy wykładzinę podłogową. Przewidywany czas prac 14 dni. Po zakończeniu prac związanych z podłogą Wykonawca dokona montażu sprzętu wraz z instalacją oprogramowania i konfiguracją sprzętu.

Okres gwarancji na prace i użyte materiały 36 miesięcy.