Załącznik nr 1 do SWZ

Szczegółowy opis przedmiotu zamówienia

I. Stacja robocza – 6 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Typ	Komputer stacjonarny.
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, aplikacji graficznych, dostępu do internetu oraz poczty elektronicznej
Wydajność	Oferowany komputer musi osiągać w teście wydajności SYSMARK 25 Overall Rating, wynik 1300 pkt. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.).
Pamięć RAM	16GB DDR4 2666MHz. Możliwość rozbudowy do 64GB. Jeden slot DIMM wolny;
Pamięć masowa	Dysk PCIe SSD 256GB PCIe NVMe Obudowa musi umożliwiać montaż dodatkowego dysku 2.5” lub 3.5”.
Grafika	Osiągająca w teście PassMark Average 3D Mark 1200 punktów
Wyposażenie multimedialne	Karta dźwiękowa czterokanałowa zintegrowana z płytą główną, zgodna z High Definition. Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie port combo, na tylnym panelu min. port audio line out.
Obudowa	Z obsługą kart o niskim profilu, umożliwiająca montaż 1 x dysku 3.5” lub 1 x dysku 2.5” wewnątrz obudowy. Napęd optyczny zamontowany w dedykowanej wnęce zewnętrznej 5.25”; Obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej. Suma wymiarów obudowy nieprzekraczająca 70 cm; Na panelu przednim zamontowany filtr powietrza chroniący wnętrze przed kurzem, pyłem itp. Filtr demontowany bez użycia narzędzi. Zasilacz o mocy 180W pracujący w sieci 230V 50/60Hz prądu zmiennego; Musi pozwalać na demontaż kart rozszerzeń bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych). Musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych) oraz posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym. Musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki; Wbudowany wizualny system diagnostyczny oparty o sygnalizację LED służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, Sygnalizacja musi być oparta na zmianie statusów diody LED; System musi być usytuowany na przednim panelu. System diagnostyczny musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię BIOS’u, awarię procesora. System diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego. Komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS.
Bezpieczeństwo	Ukryty w laminacie płyty głównej 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. System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. System zapewniający pełną funkcjonalność, a także zachowujący interfejs graficzny nawet w przypadku braku dysku twardego oraz jego uszkodzenia, nie wymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej.

BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych, odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie i ilości rdzeni oraz prędkości zainstalowanego procesora, pojemności zainstalowanych dysków twardych, wszystkich urządzeniach podpiętych do portów SATA na płycie głównej, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio. Do odczytu wskazanych informacji nie mogą być stosowane rozwiązania oparte o pamięć masową i zaimplementowane poza systemem BIOS narzędzia, np. system diagnostyczny, dodatkowe oprogramowanie. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń, możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym zdefiniowanym haśle administratora. Możliwość ustawienia haseł użytkownika i administratora składających się z cyfr, małych liter, dużych liter oraz znaków specjalnych. Możliwość włączenia/wyłączenia kontrolera SATA; Możliwość ustawienia portów USB w trybie „no BOOT" (podczas startu komputer nie wykrywa urządzeń bootujących typu USB). Możliwość wyłączania portów USB pojedynczo. Możliwość dokonywania backup'u BIOS wraz z ustawieniami na dysku wewnętrznym. Funkcja włączająca przypomnienie o konieczności oczyszczenia lub zastąpienia filtra powietrza;i Oferowany BIOS musi posiadać menu szybkiego boot'owania które umożliwia.: uruchamianie systemu zainstalowanego na dysku twardym, uruchamianie systemu z urządzeń zewnętrznych, uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, uruchomienie graficznego systemu diagnostycznego, wejście do BIOS, upgrade BIOS.
Wirtualizacja	Sprzętowe wsparcie wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głowej oraz w BIOS systemu; Możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu;
Certyfikaty i standardy	Komputer musi być wyprodukowany zgodnie z normami ISO9001 i ISO50001
Wbudowane porty	1 x HDMI 1.4, 1 x DisplayPort, port audio typu combo (słuchawka/mikrofon) na przednim panelu panelu, port audio-out na tylnym panelu obudowy, 1xRJ-45, czytnik kart pamięci SD na przednim panelu, 8 portów USB wyprowadzonych na zewnątrz obudowy, w układzie po 4 x USB z tyłu z przodu ztyłu, z czego po 2 x USB 3.2 z przodu i z tyłu; Wymagana ilość i rozmieszczenie na zewnątrz obudowy portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych; Porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej. Karta sieciowa 10/100/1000 zintegrowana z płytą główną, wspierająca obsługę WoL; Płyta główna musi być wyposażona w: 1 x PCIe x16 Gen.3, 1 x PCIe x1, 2 x DIMM z obsługą do 64 GB DDR4 RAM, 2 x SATA w tym min. 1 szt SATA 3.0. Złącze M.2 dla dysków oraz złącze M.2 bezprzewodowej karty sieciowej. Klawiatura USB w układzie polski programisty Mysz optyczna USB z dwoma przyciskami oraz rolką (scroll) Wbudowana nagrywarka DVD +/-RW
Wsparcie techniczne	Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia danych o urządzeniu na jednej witrynie internetowej producenta, w tym co najmniej: automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego;
Warunki gwarancji i serwisu	3-letnia gwarancja producenta świadczona na miejscu u klienta Czas reakcji serwisu, do końca następnego dnia roboczego. Oferent musi posiadać ISO 9001 i ISO27001 na serwis rozwiązań informatycznych
System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego

	3. Interfejs użytkownika dostępny w języku polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z poziomów: menu, otwartego okna systemu operacyjnego; 7. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 8. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 9. Graficzne środowisko instalacji i konfiguracji w języku polskim 10. Wbudowany system pomocy w języku polskim. 11. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 12. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora Zamawiającego. 13. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 14. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, w tym możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 15. Zabezpieczony hasłem hierarchiczny dostęp do systemu; 16. Konta i profile użytkowników zarządzane zdalnie; 17. Praca systemu w trybie ochrony kont użytkowników. 18. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze; 19. Molliwość zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 20. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na serwerze plików z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika 21. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 22. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 23. Oprogramowanie dla tworzenia kopii zapasowych (Backup); 24. Automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 25. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 26. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 27. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu); 28. Wbudowany mechanizm wirtualizacji typu hypervisor; 29. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem interfejsu graficznego. 30. Bezpłatne biuletyny bezpieczeństwa związane z działaniem systemu operacyjnego. 31. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; 32. Zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 33. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny; 34. Zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej i udostępnianiem plików; 35. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. 36. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi i niezarządzanymi. 37. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne; 38. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 39. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych; 40. Możliwość tworzenia wirtualnych kart inteligentnych. 41. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 42. Wsparcie dla IPSEC oparte na politykach; 43. Wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; 44. Mechanizmy logowania w oparciu o: a) Login i hasło, b) Karty inteligentne i certyfikaty (smartcard), c) Wirtualne karty inteligentne i certyfikaty chronione poprzez moduł TPM; 45. Umozliwiajacy pracę w domenie;

Oprogramowanie użytkowe	System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance + musi umożliwiać co najmniej: 1. Wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji, 2. Wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych, 3. Stosowanie kwarantanny 4. Wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear) 5. Skanowanie urządzeń USB natychmiast po podłączeniu, 6. Automatyczne odłączanie zainfekowanej końcówki od sieci, 7. Skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji. 8. Zarządzanie stacją kliencką poprzez zbieranie informacji co najmniej o: nazwie, producencie i modelu komputera, przynależności do grupy roboczej/domeny, szczegółach systemu operacyjnego, lokalnych kontach użytkowników, dacie i godzinie uruchomienia i ostatniego restartu komputera, parametrach sprzętowych (procesor, RAM, SN, dysk), BIOS, interfejsach sieciowych, dołączonych peryferiach. 9. Musi posiadać moduł ochrony IDS/IPS 10. Musi posiadać mechanizm wykrywania skanowania portów 11. Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów 12. Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości 13. Oprogramowanie do szyfrowania, chroniące dane na stacji za pomocą algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. 14. Pełne szyfrowanie dysków działających w oferowanych komputerach zapobiegające utracie danych z powodu utraty / kradzieży stacji roboczej. 15. Oprogramowanie musi szyfrować całą zawartość na urządzeniach przenośnych, takich jak pendrive, dyski USB i udostępniać ją tylko autoryzowanym użytkownikom. 16. Musi umożliwiać blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji; 17. Musi umożliwiać zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji. 18. Możliwość blokady zapisywania plików na zewnętrznych dyskach USB oraz możliwości uruchamiania oprogramowania z takich dysków. Blokada ta musi umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach. 19. Interfejs zarządzania musi wyświetlać monity o zbliżającym się zakończeniu licencji, a także powiadamiać o zakończeniu licencji. 20. Moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware poprzez ograniczenie możliwości modyfikowania chronionych plików, tylko do procesów systemowych oraz zaufanych aplikacji. 21. Możliwość zdefiniowania chronionych folderów zawierających wrażliwe dane użytkownika. 22. Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych ochroną any ransomware. 23. Monitorowanie krytycznych danych użytkownika zapobiegające atakom ransomware; 24. Centralna konsola zarządzająca umożliwiająca co najmniej: 25. przechowywanie danych w bazie typu SQ 26. zdalną instalację lub deinstalację oprogramowania, na pojedynczych stacjach, zakresie adresów IP lub grupie z ActiveDirectory; 27. tworzenie paczek instalacyjnych oprogramowania, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi oraz formatach dla systemów Linux 28. centralną dystrybucję uaktualnień definicji ochronnych, których źródłem będzie plik na serwerz konsoli; 29. raportowanie z prezentacją tabelaryczną i graficzną, możliwością automatycznego czyszczenia starych raportów, eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich; 30. definiowanie struktury opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji; 31. Możliwość tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera; 32. Dostęp do konsoli z dowolnego miejsca w nagłych przypadkach; 33. Możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń 34. Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach. 35. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych;

	36. System musi umożliwiać, z konsoli na serwerze, co najmniej: 37. różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie 38. przyznawanie praw dostępu dla nośników pamięci tj. USB, CD 39. regulowania połączeń WiFi i Bluetooth 40. kontrolowanie i regulowanie użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe 41. blokadę lub zezwolenia na połączenie się z urządzeniami mobilnymi 42. blokowanie dostępu dowolnemu urządzeniu 43. tymczasowe dodanie dostępu do urządzenia przez administratora 44. szyfrowanie zawartości USB i udostępnianie jej na stacjach końcowych; 45. zablokowanie funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszk 46. zezwalanić na dostęp tylko urządzeniom wcześniej dodanym przez administratora 47. używanda tylko zaufanych urządzeń sieciowych; 48. Funkcja wirtualnej klawiatury 49. Możliwość blokowania każdej aplikacji , w tym w oparciu o kategorie 50. Możliwość dodania własnych aplikacji do listy zablokowanych 51. Tworzenie listy aplikacji zainstalowanych na komputerach klientach poprzez konsolę administracyjną na serwerze 52. Kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool 53. Możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki; 54. Możliwość zablokowania funkcji Printscreen 55. Monitorowanie przesyłu danych między aplikacjami; 56. Monitorowanie i kontrola przepływu poufnych informacji 57. Blokowanie plików w oparciu o ich rozszerzenie lub rodzaj 58. Monitorowanie i zarządzanie danymi udostępnianymi poprzez zasoby sieciowe; 59. Ochrona przed wyciekiem informacji na drukarki lokalne i sieciowe 60. Ochrona zawartości schowka systemu 61. Ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL 62. Dodawanie wyjątków dla domen, aplikacji i lokalizacji sieciowych 63. Ochrona plików zamkniętych w archiwach 64. Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem 65. Możliwość tworzenia profilu DLP dla każdej polityki 66. Wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania 67. Ochrona przez wyciekiem plików poprzez programy typu p2p 68. Monitorowanie działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych. 69. Monitorowanie określonych rodzajów plików. 70. Możliwość wykluczenia określonych plików/folderów z procedury monitorowania. 71. Możliwość śledzenia zmian we wszystkich plikach 72. Możliwość śledzenia zmian w oprogramowaniu zainstalowanym na stacjach roboczych; 73. Możliwość definiowana własnych typów plików 74. Usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku 75. Optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem 76. Możliwość zaplanowania optymalizacji na wskazanych stacjach klienckich 77. System ochrony i zarządzania urządzeniami za pomocą platformy w chmurze;. 78. Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi 79. Musi posiadać możliwość eksportu danych użytkownika 80. Import listy urządzeń z pliku CSV 81. Dodawanie urządzeń; 82. Podgląd co najmniej następujących informacji konfiguracji: data i status wdrożenia, status urządzenia, numer telefonu, właściciel, grupa, reguły, wersja agenta 83. Podgląd co najmniej następujących informacji sprzętowych: model, producent, system, adres MAC, bluetooth, wolna przestrzeń na dysku, całkowita przeszłość na dysku, użycie procesora,; 84. Podgląd zainstalowanych aplikacji; 85. Moduł raportowania aktywności, skanowania oraz naruszenia reguł; 86. Oprogramowanie pozwalające na wykrywanie oraz zarządzanie podatnościami bezpieczeństwa dostępne przez przeglądarkę internetową; 87. Portal zarządzający w postaci SaaS; 88. Skanowanie podatności za pomocą nodów skanujących; 89. Nody skanujące w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie 90. Portal zarządzający musi umożliwiać: 91. przegląd wybranych danych;

	92. zablokowanie możliwości zmiany konfiguracji; 93. zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów; 94. tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności 95. eksport skanów podatności do pliku CSV; 96. **D**eduplikacja danych na źródle, 97. Backup przyrostowy i różnicowy, 98. Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji, 99. Backup danych lokalnych – plikowy oraz poczty; 100. Backup otwartych plików; 101. Filtr plików oraz folderów, 102. Domyślne wykluczenia zbędnych plików 103. Przywracanie danych do wskazanej lokalizacji, 104. Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora, 105. Wyszukiwanie plików w repozytorium użytkownika, 106. Automatyczne logowanie, 107. Zapamiętywanie danych logowania, 108. Automatyczne uruchamianie programu przy starcie systemu, 109. Ustawianie priorytetu dla procesu backupu, 110. Zmiana klucza szyfrującego, 111. Konfiguracja wydajności procesu backupu, 112. Zastępowanie nazwy pliku GUID-em, 113. Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika, 114. Kompresja danych, 115. Transmisja po bezpiecznym protokole TLS, 116. Deklaracja klucza szyfrującego dane użytkownika, 117. Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji, 118. Obliczanie sumy kontrolnej, 119. Kopie zapasowe musza być przechowywane w data center, na terenie Polski. 120. Licencje muszą być przypisywane do urządzenia z limitem pojemności przestrzeni w chmurze minimum 50 GB; 121. Wsparcie techniczne, świadczone w języku polskim; 122. Monitorowanie komputera i generowanie zgłoszeń o błędach / nieprawidłowym działaniu w zakresie pracy komponentów i wydajności systemów 123. Powiadamianie o nowych wersjach sterowników i umożliwienie użytkownikowi wykonania upgrade systemu 124. Powiadamianie o problemach wydajnościowych i diagnozowanie / rozwiązywanie takich problemów 125. Śledzenie kluczowych komponentów i przewidywanie awarii przed ich wystąpieniem. 126. Upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji; 127. Mozliwość sprawdzenia każdego sterownika, aplikacji, BIOS'u bezpośrednio na stronie producenta przed instalacją oraz uzyskanie informacjio: a. poprawkach i usprawnieniach dotyczących aktualizacji b. dacie wydania ostatniej aktualizacji c. priorytecie aktualizacji d. zgodności z systemami operacyjnymi e. jakiego sprzętu dotyczy aktualizacja 128. Uzyskanie wylazu najnowszych aktualizacji z podziałem na krytyczne, rekomendowane i opcjonalne 129. Włączenie/wyłączenie funkcji automatycznego restartu; 130. Rozpoznanie modelu oferowanego komputera, numeru seryjnego, uzyskanie informacj kiedy dokonany został ostatnio upgrade; 131. Sprawdzenie historii upgrade'ów z informacją jakie sterowniki były instalowane; 132. Uzyskanie wykazu wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji; 133. Uzyskanie raportu uwzględniającego informacje o : sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach, zainstalowanych aktualizacjach

II. Monitor – 2 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne

Rozmiar ekranu	23,8 cala;
Typ panelu	IPS, anti glare;
Format obrazu	16:9
Wielkość piksela	Maksymalnie 0,28
Rozdzielczość	1920 x 1080
Czas reakcji matrycy	Maksymalnie 5 ms.
Jasność	250 nitów;
Kontrast statyczny	1000:1
Głośniki	2 x 2W;
Tilt	od -5 do 20 stopni;
Katy widzenia	• 178 stopni;
Złącza	1 x VGA, 1 x HDMI, wejście mikrofonowe, wyjście słuchawkowe;
Warunki gwarancji	3 lata;
Wymagania dodatkowe	Kensington Lock, zgodność ze standardem VESA, kabel HDMI;

III. Oprogramowanie biurowe Typ I – 28 szt.

Kompletny pakiet oprogramowania biurowego musi spełniać następujące wymagania, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Wymagania odnośnie interfejsu użytkownika:
   a) Pełna polska wersja językowa interfejsu użytkownika;
   b) Prostota i intuicyjność obsługi, pozwalająca na prace osobom nieposiadającym umiejętności technicznych;
   c) Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej musi być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się;
2. Oprogramowanie musi umożliwiać tworzenie i edycje dokumentów elektronicznych w formacie, który spełnia następujące warunki:
   a) posiada kompletny i publicznie dostępny opis formatu,
   b) ma zdefiniowany układ informacji w postaci XML zgodnie z Tabela B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)
   c) umożliwia wykorzystanie schematów XML
   d) wspiera w swojej specyfikacji podpis elektroniczny zgodnie z Tabela A.1.1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)
3. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb użytkownika oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców;
4. W skład oprogramowania muszą wchodzić narzędzia umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami;
5. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim;.
6. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
   a) Edytor tekstów
   b) Arkusz kalkulacyjny
   c) Narzędzie do przygotowywania i prowadzenia prezentacji/ tworzenia, edytowania i wyświetlania prezentacji
   d) Narzędzie do zarzadzania informacja prywatną (poczta elektroniczna, kalendarzem, kontaktami i zadaniami)
7. Edytor tekstu musi umożliwiać:
   a) Edycję i formatowanie tekstu w języku polskim wraz z obsługa języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty
   b) Wstawianie oraz formatowanie tabel
   c) Wstawianie oraz formatowanie obiektów graficznych
   d) Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne)
   e) Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków
   f) Automatyczne tworzenie spisów treści
   g) Formatowanie nagłówków i stopek stron
   h) Sprawdzanie pisowni w języku polskim
   i) Śledzenie zmian wprowadzonych przez użytkowników
   j) Nagrywanie, tworzenie i edycje makr automatyzujących wykonywanie czynności
   k) Określenie układu strony (pionowa/pozioma)
   l) Wydruk dokumentów
   m) Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarzadzania informacją prywatną
   n) Prace na posiadanych przez zamawiającego dokumentach utworzonych przy pomocy Microsoft Word 2010, 2013 i 2016 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu

o) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
p) Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostepniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem.
q) Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.
r) Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostepniającego formularze i pozwalające zapisać plik wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i Prawnych.

8. Arkusz kalkulacyjny musi umożliwiać:
   a) Tworzenie raportów tabelarycznych
   b) Tworzenie wykresów liniowych (wraz linia trendu), słupkowych, kołowych
   c) Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
   d) Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)
   e) Obsługę kostek OLAP oraz tworzenie i edycje kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiazywanie problemów optymalizacyjnych
   f) Tworzenie raportów tabeli przestawnych umożliwiających dynamiczna zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych
   g) Wyszukiwanie i zamianę danych
   h) Wykonywanie analiz danych przy użyciu formatowania warunkowego
   i) Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
   j) Nagrywanie, tworzenie i edycje makr automatyzujących wykonywanie czynności
   k) Formatowanie czasu, daty i wartości finansowych z polskim formatem
   l) Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
   m) Zachowanie pełnej zgodności z formatami posiadanych przez zamawiającego plików utworzonych za pomocą oprogramowania Microsoft Excel 2010, 2013 i 2016 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń..
   n) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
9. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać przygotowywanie prezentacji multimedialnych oraz:
   a) Prezentowanie przy użyciu projektora multimedialnego
   b) Drukowanie w formacie umożliwiającym robienie notatek
   c) Zapisanie w postaci tylko do odczytu.
   d) Nagrywanie narracji dołączanej do prezentacji
   e) Opatrywanie slajdów notatkami dla prezentera
   f) Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
   g) Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
   h) Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
   i) Tworzenie animacji obiektów i całych slajdów
   j) Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera
   k) Pełna zgodność z formatami plików posiadanych przez zamawiającego, utworzonych za pomocą oprogramowania MS PowerPoint 2010, 2013 i 2016.
10. Narzędzie do zarzadzania informacja prywatna (poczta elektroniczna, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
   a) Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego
   b) Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców
   c) Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną
   d) Automatyczne grupowanie poczty o tym samym tytule
   e) Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczna do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy
   f) Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia
   g) Zarzadzanie kalendarzem
   h) Udostępnianie kalendarza innym użytkownikom
   i) Przeglądanie kalendarza innych użytkowników
   j) Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach
   k) Zarzadzanie lista zadań
   l) Zlecanie zadań innym użytkownikom
   m) Zarzadzanie listą kontaktów
   n) Udostępnianie listy kontaktów innym użytkownikom
   o) Przeglądanie listy kontaktów innych użytkowników
   a) Możliwość przesyłania kontaktów innym użytkowników
11. Licencja niewygasająca do użytku komercyjnego. Nie dopuszcza się licencji w modelu subskrypcyjnym;

IV. Oprogramowanie serwerowe – 1 szt.

Musi spełniać następujące wymagana:

1. Możliwość pracy jako kontroler domeny;;
2. Agregowanie fizycznej pojemności różnych dysków twardych;
3. Dynamicznie dodawanie dysków twardych i tworzenie wolumenów o określonych poziomach odporności;
4. Wykonywanie kopii zapasowych system operacyjnego i przywracanie bare-metal samego serwera, a także komputerów klienckich podłączonych do sieci;
5. Możliwość wyłączenia mechanizmu backupu i użycia w tym celu aplikacji firm trzecich;
6. Obsługa woluminów większych niz 2 TB;
7. Zarządzanie i konfigurowanie historii plików z komputerów klienckich;
8. Pomoc użytkownikom w odzyskiwania przypadkowo usuniętych lub zastąpionych plików bez pomocy administratora;
9. Automatycznie buforowanie plików w celu uzyskania dostępu w trybie offline i synchronizowanie podczas połączenia z serwerem;
10. Kreator konfigurowania VPN;
11. Monitorowanie poprawności działania systemów operacyjnych komputerów klienckich i serwera;
12. Monitorowanie problemów związanych z kopiami zapasowymi komputerów klienckich, pamięcią masową serwera, małą ilością miejsca na dysku;
13. Tworzenie obrazów systemu i zainstalowanych aplikacji;
14. Tworzenie bootowalnego USB;
15. Możliwość konfiguracji do obsługi sieci bezprzewodowej;
16. Zbior narzedzi i plików binarnych oraz pakietów językowych ułatwiających wdrożenie (ADK);
17. Możliwosc konfigurowania partycji;
18. Narzędzie do tworzenia zestawu plików, które służą do definiowania listy nazw domen;
19. Optymalizacja rozdzielczości strumieniowego przesyłania wideo.;
20. Ukrywanie dodatku do zdalnego strumieniowania multimediów
21. Ustawianie nazwy biblioteki multimediów
22. Ustawianie jakości przesyłania strumieniowego wideo wraz zjego włączaniem i wyłączaniem;
23. Programowo włączanie lub wyłączanie strumieniowego przesyłania multimediów
24. Ustawianie kolejności kart na pulpicie nawigazyjnym poprzez wpisy w rejestrach;
25. Pakiety językowe;
26. Backup online;
27. Obsługa za pomocć skryptów konfiguracyjnych;
28. Możliwość utworzenia nośnika recovery dla serwera administrowanego zdalnie;
29. Automatyczna migracja danych do i z serwerów z zainstalowanym niniejszym oprogramownaiem;
30. Przekierowywanie folderów na serwerze docelowym;
31. Musi posiadac analizator najlepszych praktyk;
32. Możliwość łączenie się z siecią organizacji z dowolnego urządzenia wyposażonego w Internet bez nawiązywania połączenia z wirtualną siecią prywatną (VPN);
33. Mozliwość przywrócenia plików, folderów lub całego serwera z kopii zapasowej be zużycia innych plikacji;
34. Backup przyrostowy;
35. Przesyłanie informacji o zmianach plikach do chmury;
36. Optymalizacja wykorzystania przepustowaości sieci LAN i WAN;
37. Backup komputerów klienckich podłączonych do sieci zmożliwościa jego konfiguracj i jego odtwarzaniei;
38. Kreator naprawy kopii zapasowej bazy danych;
39. Reset do ustawień domyślnych i czyszczenie kopii zapasowej;
40. Zarządzanie urządzeniami sieciowymi za pomocą pulpitu nawigacyjnego serwera;
41. Możliwosc stworzenia biblioteki multimediów;
42. Zarządzanie dyskami twardymi za pomocą pulpitu nawigacyjnego
43. Przeprowadzanie kontroli i napraw dysków twardych;
44. Formatowanie dysków twardych
45. Dodawanie nowego dysku twardego;
46. Licencja na 2 CPU i 64 GB RAMu;
47. Możliwość uruchomienia zarównio w postci fizycznej jak wirtualnej;

V. Dyski – 2 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Rozmiar	2,5"
Interfejs	SATA 3.0 (6Gb/s) zgodny z interfejsem SATA 2.0 (3Gb/s)
Pojemności	960 GB;
Szyfrowanie	XTS-AES z 256-bitowym kluczem
Szybkość odczytu/zapisu sekwencyjnego	560MBs/530MBs;
Narzędzia SMART	Monitorowanie niezawodności, statystyki dotyczące użycia, pozostały czas eksploatacji dysku, temperatura

Zuzycie energii	Maksymalnie 5W;
Wibracje podczas pracy	Maksymalnie 20G;
MTBF	2 mln. godzin;
Gwarancja	5 lat;
Wymagania dodatkowe	Wymiana podczas pracy, statyczne i dynamiczne równoważenie zużycia,

VI. **Szafa krosowa – Typ I – 1 szt.**

1. Rack 19”
2. Wysokość - 32U;
3. Szerokość - 600 mm
4. Głębokość - 600 mm
5. Otwory wentylacyjne w dachu i w podłodze do wentylacji grawitacyjnej oraz do opcjonalnego zamontowania wentylatorów z termostatem lub bez;
6. Perforacja na drzwiach
7. Zdejmowane panele boczne umożliwiające wygodny dostęp do urządzeń
8. Możliwość zamontowania opcjonalnych zamków w panelach bocznych;
9. 4 szyny Rack zapewniające bezpieczny montaż większych urządzeń oraz dające możliwość zamontowania mniejszych urządzeń w 2 płaszczyznach;
10. Możliwość zamontowania drzwi jako prawe lub lewe
11. Kat otwarcia drzwi – 220 stopni;
12. Drzwi przednie szklane z hartowanego szkła;
13. Drzwi tylne pełne, stalowe lub perforowane;
14. Otwory w podłodze i dachu do wprowadzenia przewodów
15. Zamek drzwi przednich i tylnych
16. Możliwość zamontowania cokołów;
17. Stalowa blacha zimnowalcowana
18. Grubość blachy ramy: 1,5 mm;
19. Grubość blachy paneli bocznych: 1,2 mm;
20. Grubość blachy szyn montażowych aack: 2,5 mm
21. Grubość szkła: 5 mm;
22. Nośność: 800 kg
23. Drzwi przednie: szklane z klamką i zamkiem
24. Drzwi tylne: stalowe pełne z zamkiem
25. Waga: maksymalnie 70 kg
26. Normy wykonania: ANSI/EIA RS-310-D, DIN41491 PART1, IEC297-2, DIN41494 PART7, GB/T3047.2-92
27. Kompatybilność ze standardami: metrycznym ETSI oraz międzynarodowym 19”
28. Szafa złożona zapakowana na palecie;
29. Śruby rack do montażu elementów w szafie - 25 kpl.
30. Koła z blokadami - 4szt
31. Regulowane nóżki - 4szt
32. Kompatybilna listwa zasilająca:
    a) Typ gniazda wejściowego: Kabel z wtykiem PL (16A)
    b) Liczba gniazd wyjściowych: 8 szt.
    c) Liczba gniazd zasilających 10A PL: 8 szt.
    d) Długość przewodu zasilającego: 1.8 metr
    e) Napięcie znamionowe: 230 V AC
    f) Prąd znamionowy: 16 A;
    g) Możliwość zamontowania w szafie rack 19";
33. Kompatybilny panel wentylacyjny do szaf RACK z termostatem cyfrowym;

VII. Szafa krosowa – Typ II – 1 szt.

1. Wysokość - 27U;
2. Szerokość - 600 mm
3. Głębokość - 600 mm
4. Nośność– 800 kg.;
5. Przeszklone drzwi;
6. Drzwi boczne zatrzaskowe z zamknięciem na klucz I możliwością demontażu;
7. Otwory na przewody w ścianie dolnej i górnej;

8. Drzwi tylne zamykane na klucz;
9. Otwory wentylacyjne w drzwiach i ścianach bocznych;
10. Możliwość zamontowania dwóch wentylatorów w suficie;
11. W komplecie dwa zestawy kluczy;
12. Możliwość regulacji pionowych szyn, które można ustawiać co ćwierć cala;
13. Nóżki poziomujące oraz cztery kółka w tym dwa z hamulcem;
14. Szafa musi być produkowana zgodnie z norma ISO 9001;
15. Półka o nośności 20 kilogramów i wysokości 1U;
16. Pólka musi być wykonana z perforowanej blachy wykończonej w kolorze czarnym lub jasnoszarym;
17. Półka musi posiadać otwory montażowe i komplet śrub oraz koszyczków;
18. Panel wentylacyjny z 2 wentylatorami montowany w górnej płycie;
19. Panel musi być montowany czteropunktowao i posiadac kabel zasilający o długości 1,3m.;
20. Gwarancja na panel – 24 miesiące;
21. Listwa zasilająca o wysokości 1U z 8 gniazdami Schuko;
22. Listwa musi być mocowana doczołowo w 6 punktach;
23. Przewód zasilający w listwie o długości – 1,8m.;
24. Termostat zamykający 10A z regulacja temperatury od 0 do 60 stopni Celsjusza;;
25. Pobór mocy termostatu – maksymalnie 30W;
26. Stopien ochorny termonstatu – IP20;
27. Maksymalna zdolność przełączania - 120V@15A, 230V@10A, 250V@10A;
28. Ognioodporność - UL 94 V-0;
29. Gwarancja na szafę – 3 lata;

VIII. Przełącznik sieciowy – Typ I – 2 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Wydajność w (pakiety 64-bajtowe)	75 mpps
Zdolność przełączania	100 Gb/s
Spanniny Tree Protocol (STP)	Obsługa STP 802.1d Szybka konwergencja przy użyciu 802.1w (RSTP) 8 Instancji MSTP przy użyciu protokołu 802.1s 126 instancji PVST+ i 126 RPVST+;
Grupowanie portów / agregacja łączy	Obsługa protokołu IEEE 802.3ad (LACP) 4 grupy 8 portów na grupę z 16 portami na każdą grupę 802.3ad
VLAN	Obsługa 250 aktywnych sieci VLAN jednocześnie; Sieci VLAN oparte na portach i znacznikach 802.1Q; Gościnna sieć VLAN; Mozliwość zarządzania sieciami VLAN;
Voice VLAN	Ruch głosowy musi być automatycznie przypisywany do sieci VLAN dedykowanej dla niego i traktowany z odpowiednimi poziomami QoS; VSDP dla urządzeń do sterowania połaczeniami w sieci;
GARP i GVRP	Protokoły do automatycznej propagacji i konfiguracji sieci VLAN w domenie;
Wykrywanie sprzężenia zwrotnego	Musi zapewniać ochronę przed pętlami, przesyłając pakiety protokołu pętli poza porty, na których włączono ochronę przed pętlami. Musi działać niezależnie od STP;
Routing IPv4	32 trasy statyczne i 16 interfejsów IP;
Routing IPv6	Z prędkością łącza
Interfejs warstwy 3	Konfiguracja interfejsu warstwy 3 na porcie fizycznym, interjejsie LAG, VLAN lub pętli zwrotnej;
DHCP	Przekazywanie ruchu DHCP w domenach IP;
SSL	Musi szyfrować cały ruch HTTPS, umożliwiając bezpieczny dostęp do graficznego interfejsu zarządzania opartego na przeglądarce;
SSH	Obsługa SSH v1 i v2;
IEEE 802.1X	Zdalne uwierzytelnianie; Uwierzytelnianie RADIUS; tryb jednego/wielu hostów;
SCT	Musi zapewniać odbieranie i przetwarzanie ruchu związanego z zarządzaniem i protokołami, niezależnie od tego, jak duży ruch jest odbierany;

UDP	Przekazywanie informacji rozgłoszeniowych w domenach warstwy 3 w celu wykrywania aplikacji lub przekazywania pakietów BOOTP / DHCP
SSD	Zarządzanie poufnymi danymi takimi jak hasła, klucze; Umieszczanie tych danych na innych urządzeniach i bezpiecznej automatycznej konfiguracji; Dostęp do przeglądania poufnych danych w postaci zwykłego tekstu lub zaszyfrowanych musi być zapewniony zgodnie z poziomem dostępu skonfigurowanym przez użytkownika;
Bezpieczeństwo portu	Możliwość zablokowania źródłowych adresów MAC na portach i ograniczenia liczby poznanych adresów MAC;
ACL	Obsługa 512 reguł Limit odrzucania lub szybkości w oparciu o źródłowy i docelowy adres MAC, VLAN ID lub adres IPv4 lub IPv6, etykietę przepływu IPv6, protokół, port, priorytet DSCP/IP, porty źródłowe i docelowe TCP/UDP, priorytet 802.1p, pakiety ICMP i IGMP; ACL możliwy do stosowania zarówno po stronie wejściowej, jak i wyjściowej Obsługa list ACL opartych na czasie;
QoS	8 kolejek sprzętowych
IPv6	Tryb hosta IPv6 IPv6 przez Ethernet Podwójny stos IPv6/IPv4 Automatyczna konfiguracja adresu IPv6 Wykrywanie maksymalnej jednostki transmisji ścieżki (MTU) Wykrywanie zduplikowanych adresów (DAD) IPv4 z obsługą ISATAP;
Interfejs uzytkownika	Wbudowane narzędzie do konfiguracji przełączników umożliwiające konfigurację urządzeń w przeglądarce; Obsługa konfiguracji, kreatorów, pulpitu nawigacyjnego systemu, konserwacji i monitorowania systemu;
RMON	Wbudowany agent oprogramowania obsługujący co najmniej 4 grupy RMON w celu usprawnienia zarządzania ruchem, monitorowania i analizy;
Dublowanie portów	Ruch na porcie musi być dublowany do innego portu w celu analizy za pomocą analizatora sieci lub sondy RMON; Mozliwośść zdublowania do jednego portu docelowego 4 portów źródłowych;
Dublowanie sieci VLAN	Dublowanie do portu w celu analizy za pomocą analizatora sieci lub sondy RMON; Mozliwość zdublowania do jednego portu docelowego 4 źródłowych sieci VLAN;
CLI	Skryptowalny, obsługa pełnego CLI, a także opartego na menu;
PoE	Zasilanie PoE włączane lub wyłączane na podstawie harmonogramu zdefiniowanego przez użytkownika;
Ramki jumbo	Rozmiary ramek do 9K bajtów;
Tabela MAC	8 tys. adresów
Rozpraszanie ciepła	840 BTU/godz.
Porty	48 x GigabiEthernet PoE, 4 x Gigabit SFP, port konsoli USB/RJ45, USB na przednim panelu;
Budzet mocy portów PoE	180W;
Procesor	800 Mhz;
Flash	256 MB;
RAM	512 MB;
Bufor pakietów	3 MB;
Poziom hałasu	Maksymalnie 40 dBA;
Wymagania dodatkowe	IGMP 1, 2 i 3, CIDR, wentylator, zestaw montażowy w szafie rack;
Gwarancja	5 lat;

IX. Przełącznik sieciowy – Typ II – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Liczba portów	28, w 24 x 1GbE i 4 x 10 GbE SFP+;
Zdolność przełączania	128 Gbps.
Szybkość przekazywania	95 Mbp/s
Bufor pakietów	1,5 mln. bajtów;

Tabela adresów MAC	16 tys.
Tabela przekazywania L3	512 wpisów IPv4 i 512 wpisów IPv6;
Tabela routingu	32
Intersejsy IPv4 i IPv6	32/32;
Flash	32 MB;
RAM	512 MB;;
Pobór mocy	Maksymalnie 25W;
Zgodnośc ze standardami	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Ethernet IEEE 802.3ab 1000BASE-T Ethernet IEEE 802.3z 1000BASE-X IEEE 802.3ae 10-Gigabit Ethernet IEEE 802.3af PoE IEEE 802.3at PoE Plus IEEE 802.3az EEE Kontrola przepływu IEEE 802.3x Agregacja LACP IEEE 802.3ad* IEEE 802.1D (STP) IEEE 802.1w (RSTP) IEEE 802.1s (MSTP) Priorytetyzacja klasy usług (CoS) IEEE 802.1p Uwierzytelnianie portu IEEE 802.1X*
Kontrola ruchu	VLAN* 802.1Q/1K/4K Obsługa do 4K VLAN ID Niezależne uczenie się sieci VLAN (IVL) L2PT VLAN oparty na portach Głosowa sieć VLAN Trunking VLAN GVRP
Bezpieczeństwo	802.1X Uwierzytelnianie MAC Statyczne przekierowanie MAC SSL Statyczny ARP Filtrowanie bezpieczeństwa oparte na zasadach Izolacja portu Wyszukiwanie MAC Gościnna sieć VLAN Agent przekazujący PPPoE PPPoE IA i 82 Włączenie/wyłączenie pułapek związanych z interfejsem Certyfikacja SHA2 HTTPS Uwierzytelnianie logowania przez RADIUS Autoryzacja na RADIUS 802.1x VLAN i przydzielanie przepustowości przez RADIUS* Filtrowanie pakietów ACL;
QoS	Liczba kolejek sprzętowych na port: 8 Metody kolejkowania 802.1p: SPQ, WRR, WFQ Ograniczenie szybkości na port Ograniczanie transferu w oparciu o zasady Priorytetyzacja w oparciu o politykę
Multicast w warstwie 2	Grupa multicast L2: 1K Śledzenie IGMP v1, v2, v3 Konfigurowalny zegar i priorytet IGMP snooping Ograniczanie IGMP Filtrowanie IGMP Multicast statyczny
Routing	Przekaźnik DHCP ze źródłowym interfejsem IP
Zarządzanie	SNMP v1, v2c, v3 RMON Dziennik systemowy IPv4/v6 IEEE 802.1AB LLDP IEEE 802.1AB LLDP-MED
Zarządzanie IPv6	IPv6 przez Ethernet;)

	Architektura adresowania IPv6; Podwójny stos; ICMPv6; Ścieżka MTU; Przekaźnik DHCPv6 Domyślny tryb klienta DHCP Wykrywanie zduplikowanych adresów (DAD)
Zarządzanie urządzeniami	Zarządzanie przez interfejs WWW, Telnet, Internet, SNMP Zarządzanie chmurą; Kreator konfiguracji Aktualizacja oprogramowania przez FTP/Web Zapisywanie i pobieranie konfiguracji Obsługiwane wielokrotne logowanie Klonowanie konfiguracji Przekaźnik DHCP na VLAN Klient DHCP IPv4, IPv6 Serwer NTP obsługujący format DNS Dublowanie portów Przywracanieóć do ostatniego ustawienia domyślnego;
MTBF	1 200 000 godzin
Rozpraszanie ciepła	80 BTU/hr
Poziom hałasu	Maksymalnie 0 dB;
Wymagania dodatkowe	Zestaw montażowy w szafie rack,
Gwarancja	5 lat;

X. Serwer Typ I – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	Rack o wysokości max 1U z możliwością instalacji 4 dysków 3,5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych bez organizera do kabli.
Płyta główna	Zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym; Musi obsługiwać 128GB RAM; Musi posiadać 4 sloty przeznaczone dla pamięci
Procesor	Osiągający w teście PassMark CPU Mark wynik 15 400 – załączyć do oferty wydruk ze strony https://www.cpubenchmark.net/
RAM	2 x 16GB o częstotliwości pracy 3200MT/s.
Zabezpieczenia pamięci RAM	Mechanizm oszczędzania, mirror pamięcui, izolowanie uszkodzonych gniazd DIMM, ochorna parzystości, ograniczanie temperatury kości;
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość. 1920 x 1200
Wbudowane porty	4 porty USB w tym 1 port USB 3.0 z tyłu obudowy, 1 port VGA na tylnym panelu, 1 port RS232
Gniazda PCI	3 sloty PCIe generacji 4
Interfejsy sieciowe	Wbudowane 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT. Porty nie mogą być osiągnięte poprzez karty w slotach PCIe;
Kontroler dysków	Sprzętowy kontroler dyskowy SATA 6Gb/s / SAS 12Gb/s / PCIe 4.0 (NVMe); 8GB Cache; Wymagane konfiguracje poziomów RAID: 0, 1, 10, 6, 5; Wsparcie dla dysków samoszyfrujących.
Dyski twarde	Możliwość instalacji dysków SAS, SATA, SSD, NL SAS Zainstalowane 2x 900GB SAS 12Gbps 15k. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności 480GB Hot-Plug z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w 2 nośniki typu flash o pojemności 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera. Rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
System diagnostyczny	Diody LED informujące o kondycji serwera + panel lcd
Wentylatory	4 wentylatory
Zasilacze	Dwa zasilacze o mocy maksymalnej 600W.
System operacyjny	Musi spełniać następujące wymagana: 1. Możliwość pracy jako kontroler domeny;; 2. Agregowanie fizycznej pojemności różnych dysków twardych;

	3. Dynamicznie dodawanie dysków twardych i tworzenie wolumenów o określonych poziomach odporności; 4. Wykonywanie kopii zapasowych system operacyjnego i przywracanie bare-metal samego serwera, a także komputerów klienckich podłączonych do sieci; 5. Możliwość wyłączenia mechanizmu backupu i użycia w tym celu aplikacji firm trzecich; 6. Obsługa woluminów większych niz 2 TB; 7. Zarządzanie i konfigurowanie historii plików z komputerów klienckich; 8. Pomoc użytkownikom w odzyskiwania przypadkowo usuniętych lub zastąpionych plików bez pomocy administratora; 9. Automatycznie buforowanie plików w celu uzyskania dostępu w trybie offline i synchronizowanie podczas połączenia z serwerem; 10. Kreator konfigurowania VPN; 11. Monitorowanie poprawności działania systemów operacyjnych komputerów klienckich i serwera; 12. Monitorowanie problemów związanych z kopiami zapasowymi komputerów klienckich, pamięcią masową serwera, małą ilością miejsca na dysku; 13. Tworzenie obrazów systemu i zainstalowanych aplikacji; 14. Tworzenie bootowalnego USB; 15. Możliwość konfiguracji do obsługi sieci bezprzewodowej; 16. Zbior narzedzi i plików binarnych oraz pakietów językowych ułatwiających wdrożenie (ADK); 17. Możliwosc konfigurowania partycji; 18. Narzędzie do tworzenia zestawu plików, które służą do definiowania listy nazw domen; 19. Optymalizacja rozdzielczości strumieniowego przesyłania wideo.; 20. Ukrywanie dodatku do zdalnego strumieniowania multimediów 21. Ustawianie nazwy biblioteki multimediów 22. Ustawianie jakości przesyłania strumieniowego wideo wraz zjego włączaniem i wyłączaniem; 23. Programowo włączanie lub wyłączanie strumieniowego przesyłania multimediów 24. Ustawianie kolejności kart na pulpicie nawigazyjnym poprzez wpisy w rejestrach; 25. Pakiety językowe; 26. Backup online; 27. Obsługa za pomocć skryptów konfiguracyjnych; 28. Możliwość utworzenia nośnika recovery dla serwera administrowanego zdalnie; 29. Automatyczna migracja danych do i z serwerów z zainstalowanym niniejszym oprogramownaiem; 30. Przekierowywanie folderów na serwerze docelowym; 31. Musi posiadac analizator najlepszych praktyk; 32. Możliwość łączenie się z siecią organizacji z dowolnego urządzenia wyposażonego w Internet bez nawiązywania połączenia z wirtualną siecią prywatną (VPN); 33. Mozliwość przywrócenia plików, folderów lub całego serwera z kopii zapasowej be zużycia innych plikacji; 34. Backup przyrostowy; 35. Przesyłanie informacji o zmianach plikach do chmury; 36. Optymalizacja wykorzystania przepustowaości sieci LAN i WAN; 37. Backup komputerów klienckich podłączonych do sieci zmożliwościa jego konfiguracj i jego odtwarzaniei; 38. Kreator naprawy kopii zapasowej bazy danych; 39. Reset do ustawień domyślnych i czyszczenie kopii zapasowej; 40. Zarządzanie urządzeniami sieciowymi za pomocą pulpitu nawigacyjnego serwera; 41. Możliwosc stworzenia biblioteki multimediów; 42. Zarządzanie dyskami twardymi za pomocą pulpitu nawigacyjnego 43. Przeprowadzanie kontroli i napraw dysków twardych; 44. Formatowanie dysków twardych 45. Dodawanie nowego dysku twardego; 46. Licencja na 2 CPU i 64 GB RAMu; 47. Możliwość uruchomienia zarównio w postci fizycznej jak wirtualnej;
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS musi mieć możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • monitoring wszystkich kluczowych komponentów jak wentylatory, zasilacze, pamięć, procesor,

	RAID, karty sieciowe oraz dyski twarde; • informacje o aktualnym zużyciu energii oraz temperaturach • kontrola zasilania, w tym co najmniej włączenie, wyłączenie, restart • funkcje diagnostyczne: podgląd dziennika systemowego, dziennika kontrolera cyklu życia; • odtworzenie konfiguracji sprzętowej na podstawie kopii z innego serwera • możliwość skonfigurowania wielu kont o zróżnicowanym poziomie przywilejów; • szyfrowanie protokołem SSL
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-50001 Serwer musi znajdować się na ogólnodostępnej liście producenta oferowanego systemu operacyjnego, potwierdzającej kompatybilnośc oferowanego sprzętu i oprogramowania
Warunki gwarancji	5 lat gwarancji, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia; Możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Dyski w razie awarii zostają u zamawiającego Serwis musi być świadczony zgodnie z normą ISO 27001 Możliwość rozszerzenia gwarancji przez producenta do 7 lat; Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

XI. Serwer Typ II – 2 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	Obudowa Rack o wysokości maksymalnie 1U z możliwością instalacji 4 dysków 3.5" wraz z kompletem szyn umożliwiających montaż w szafie rack;
Płyta główna	Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowymoraz musi obsługiwać 128GB pamięci RAM; Na płycie głównej muszą znajdować się 4 sloty przeznaczone dla pamięci RAM;
Procesor	Osiągający w teście PassMark CPU Mark wynik 17 300
RAM	16GB GB pamięci RAM ECC UDIMM o częstotliwości pracy 3200MT/s.;
Gniazda PCI	2 sloty PCIe generacji 4
Interfejsy sieciowe	Wbudowane 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT. Porty nie mogą być osiągnięte poprzez karty w slotach PCIe;
Kontroler dyskowy	Sprzętowy kontroler dyskowy, posiadający 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfujących.
Dyski twarde	Możliwość instalacji dysków SAS, SATA, SSD, NL SAS Zainstalowane 2 dyski SAS o pojemności. 900GB każdy, 12Gb, Hot-Plug. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności 480GB z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w 2 nośniki typu flash o pojemności 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Wbudowane porty	4 porty USB w tym 1 x USB 3.0, 1 port VGA , 1 port RS232
Wentylatory	3 szt.
Zasilacz	450W
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz, służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS musi mieć możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Diagnostyka	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Karta zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • monitoring wszystkich kluczowych komponentów (wentylatory, zasilacze, pamięć, procesor,

	RAID, karty sieciowe oraz dyski twarde) • uzyskanie informacji o aktualnym zużyciu energii oraz temperaturach • kontrola zasilania (włączenie, wyłączenie, restart) • podstawowe funkcje diagnostyczne: podgląd dziennika systemowego, dziennika kontrolera cyklu życia; • odtworzenie konfiguracji sprzętowej na podstawie kopii z innego serwera • możliwość skonfigurowania wielu kont o zróżnicowanym poziomie przywilejów • szyfrowanie protokołem SSL
System operacyjny	Musi spełniać następujące wymagana: 1. Możliwość pracy jako kontroler domeny;; 2. Agregowanie fizycznej pojemności różnych dysków twardych; 3. Dynamicznie dodawanie dysków twardych i tworzenie wolumenów o określonych poziomach odporności; 4. Wykonywanie kopii zapasowych system operacyjnego i przywracanie bare-metal samego serwera, a także komputerów klienckich podłączonych do sieci; 5. Możliwość wyłączenia mechanizmu backupu i użycia w tym celu aplikacji firm trzecich; 6. Obsługa woluminów większych niz 2 TB; 7. Zarządzanie i konfigurowanie historii plików z komputerów klienckich; 8. Pomoc użytkownikom w odzyskiwania przypadkowo usuniętych lub zastąpionych plików bez pomocy administratora; 9. Automatycznie buforowanie plików w celu uzyskania dostępu w trybie offline i synchronizowanie podczas połączenia z serwerem; 10. Kreator konfigurowania VPN; 11. Monitorowanie poprawności działania systemów operacyjnych komputerów klienckich i serwera; 12. Monitorowanie problemów związanych z kopiami zapasowymi komputerów klienckich, pamięcią masową serwera, małą ilością miejsca na dysku; 13. Tworzenie obrazów systemu i zainstalowanych aplikacji; 14. Tworzenie bootowalnego USB; 15. Możliwość konfiguracji do obsługi sieci bezprzewodowej; 16. Zbior narzedzi i plików binarnych oraz pakietów językowych ułatwiających wdrożenie (ADK); 17. Możliwośc konfigurowania partycji; 18. Narzędzie do tworzenia zestawu plików, które służą do definiowania listy nazw domen; 19. Optymalizacja rozdzielczości strumieniowego przesyłania wideo.; 20. Ukrywanie dodatku do zdalnego strumieniowania multimediów 21. Ustawianie nazwy biblioteki multimediów 22. Ustawianie jakości przesyłania strumieniowego wideo wraz zjego włączaniem i wyłączaniem; 23. Programowo włączanie lub wyłączanie strumieniowego przesyłania multimediów 24. Ustawianie kolejności kart na pulpicie nawigazyjnym poprzez wpisy w rejestrach; 25. Pakiety językowe; 26. Backup online; 27. Obsługa za pomocć skryptów konfiguracyjnych; 28. Możliwość utworzenia nośnika recovery dla serwera administrowanego zdalnie; 29. Automatyczna migracja danych do i z serwerów z zainstalowanym niniejszym oprogramownaiem; 30. Przekierowywanie folderów na serwerze docelowym; 31. Musi posiadac analizator najlepszych praktyk; 32. Możliwość łączenie się z siecią organizacji z dowolnego urządzenia wyposażonego w Internet bez nawiązywania połączenia z wirtualną siecią prywatną (VPN); 33. Mozliwość przywrócenia plików, folderów lub całego serwera z kopii zapasowej be zużycia innych plikacji; 34. Backup przyrostowy; 35. Przesyłanie informacji o zmianach plikach do chmury; 36. Optymalizacja wykorzystania przepustowaości sieci LAN i WAN; 37. Backup komputerów klienckich podłączonych do sieci zmożliwościa jego konfiguracj i jego odtwarzaniei; 38. Kreator naprawy kopii zapasowej bazy danych; 39. Reset do ustawień domyślnych i czyszczenie kopii zapasowej; 40. Zarządzanie urządzeniami sieciowymi za pomocą pulpitu nawigacyjnego serwera; 41. Możliwośc stworzenia biblioteki multimediów; 42. Zarządzanie dyskami twardymi za pomocą pulpitu nawigacyjnego 43. Przeprowadzanie kontroli i napraw dysków twardych; 44. Formatowanie dysków twardych 45. Dodawanie nowego dysku twardego; 46. Licencja na 2 CPU i 64 GB RAMu;

	47. Możliwość uruchomienia zarówno w postci fizycznej jak wirtualnej;
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-50001 Serwer musi znajdować się na ogólnodostępnej liście producenta oferowanego systemu operacyjnego, potwierdzającej kompatybilnośc oferowanego sprzętu i oprogramowania
Warunki gwarancji	5 lat gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Uszkodzony dysk twardy pozostaje u Zamawiającego. Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. Serwis musi być świadczony zgodnie z normą ISO 27001
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

XII. Zasilacz awaryjny – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Rodzaj	jednofazowy
Typ obudowy	Metalowa rack 2U,tower z zestawem montażwym w szafie rack;
Topologia	Line-interactive;
Rodzaj wejścia	IEC C14;
Wyjście	10 x IEC C13 zabezpieczone przed przepięciami i bateriami;
Obciążenie krytyczne i niekrytyczne CL/NCL	5
Czas transferu	Maksymalnie 5 ms.
Przewód zasilający	1,8 m.
Moc VA/W	1000/1000
AVR	Double Boost, single buck;
Układ przecieprzepięciowy	2400J, ochrona sieci LAN (RJ45),
Czas pracy na baterii (podtrzymania)	5 minut przy pełnym obciążeniu/ 20 min. przy połowicznym;
Czas naładowania baterii	Maksymalnie 3h;
Złącza	1 x EPO, 1 x USB, 1 x port serial, 2 x RJ45;
Rozpraszanie ciepła	45 BTU/h
Hałas	Maksymalnie 55 dBA;
Warunki gwarancji	2 lata;
Wymagania dodatkowe	Kompatybilność z aktywnym PFC, obrotowy panel LCD, wewnętrzny ogranicznik prądu, bezpiecznik, uruchamianie na baterii, wbudowany moduł zarządzania akumulatorem, możliwość wymiany baterii przez użytkownika, bateria hot-swap, filtrowanie EMI/RFI, styk bezprądowy, kabel USB, szeregowy, EPO;

XIII. Pamięć RAM Typ I – DIMM DDR4 2133 16(2x8)GB - 3 szt.

XIV. Pamięć RAM Typ II –DIMM DDR3 1600 16(2x8)GB - 1 szt.

XV. Pamięć RAM Typ III – SO-DIMM 1600 8GB - 2 szt.

XVI. Monitor interaktywny – 2 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Przekatna matrycy	65 cali
Rozdzielczość ekranu	4K/UHD (3840×2160)
Czas reakcji matrycy	Maksymalnie 10 ms
Jasność	380 cd/m^2

Czas reakcji dotyku	Maksymalnie 8 ms.;
Kontrast typowy	4000:1
Żywotność matrycy	50 000 godzin
Głosniki	2 x 15W;
Szyba frontowa	Grubośc 3 mm;
Technologia dotyku	Podczerwień;
Rozdzielczość dotyku	32768 x 32768;
Złacza	3 × HDMI, 1 x VGA, 2 x audio, 4 x USB 3.0, 1 x USB 2.0, 2 x USB touch, 1 x RS 232, 2 x RJ45, 1 x USB-C;
Komunikacja bezprzewodowa	Wifi, bluetooth;
Waga	Maksymalnie 40 kg;
Zużycie energii	Maksymalnie 450 W;
Oprogramowanie	1. Oprogramowanie powinno być w języku polskim i w maksymalnym stopniu dawać możliwość wykorzystania monitora oraz dać jak największą pomoc nauczycielom w przekazaniu trudnych tematów z zakresu matematyki czy innych przedmiotów ścisłych. 2. Oprogramowanie musi zawierać narzędzia do tworzenia elektronicznych adnotacji, takich jak: - kolorowe pisaki/zakreślacze - pisaki tekstury - pióro stalówka - pióro pędzel - predefiniowane kształty (linie, strzałki, figury geometryczne) - laserowe piórko 3. Musi umożliwiać definiowanie łączy do dowolnych obiektów 4. Musi umożliwiać rozpoznawanie i konwersję rysowanych odręcznie podstawowych figur geometrycznych 5. Musi posiadać narzędzia do geometrii: skalowana linijka (stała podziałka możliwość skracania i wydłużania linijki jak taśmy mierzącej, skalowalna identycznie jak linijka ekierka, dodatkowo kątomierz i cyrkiel 6. Musi umożliwiać zmianę grubości i koloru dowolnego narysowanego obiektu, czy linii 7. Musi umożliwiać wypełnienie dowolnym kolorem zamkniętych obszarów narysowanych obiektów i kształtów 8. Musi umożliwiać pełną edycję obiektów: obrót, przesuwanie, zmiana rozmiarów, ustawianie kolejności czy grupowanie i rozgrupowanie obiektów 9. Musi posiadać edytowalną, wbudowaną galerię, zawierającą obrazki i, gotowe szablony. 10. Musi posiadać edytowalną, wbudowaną galerię grup grafik, zdjęć tematycznych oraz teł; 11. Musi umożliwiać tworzenie własnych grup graficznych z dowolnych obrazów, tak aby nauczyciel był w stanie przygotować zestaw potrzebnych grafik lub obrazów zamkniętych w jednym pliku w celu łatwego użycia podczas lekcji. 12. Musi umożliwiać eksport min. do formatu: - plików Microsoft PowerPoint 97-2019 (PPT) - plików Microsoft Word 97-2019 (DOC) - plików Microsoft Excel 97-2019 (XSL) - plików Adobe Portable Document (PDF) - plików stron internetowych (HTML) - plików CorelDraw (CDR) - plików graficznych (BMP, JPG, PNG, GIF, TIF) - plików grup graficznych tworzonych przez użytkownika - plików grup teł tworzonych przez użytkownika 13. Musi umożliwiać wstawianie plików wideo, audio 14. Musi umożliwiać wstawianie tekstu za pomocą klawiatury ekranowej 15. Musi umożliwiać rozpoznawanie i konwersję pisma odręcznego 16. Musi umożliwiać zrzuty ekranu umieszczane w środowisku pracy (zaznaczenie, cały ekran, dostępne okna aplikacji lub dowolny kształt) 17. Musi umożliwiać zakrywanie treści przy zastosowaniu kurtyny ekranowej i elektronicznego reflektora 18. Musi posiadać narzędzie pozwalające przesunąć całą zawartość grafik i tekstu jednym ruchem po całym ekranie 19. Musi posiadać zintegrowane oprogramowanie do nauk matematyczno-przyrodniczych takich jak matematyka i geometria, fizyka, chemia, elektrotechnika, mechanika

	20. Musi umożliwiać rysowanie kształtów podstawowych figur płaskich 21. Musi umożliwiać rysowanie łuków, części koła wraz z automatycznym wykreślaniem cięciw, promieni okręgów wraz z podaniem ich długości 22. Musi umożliwiać automatyczne rysowanie figur przestrzennych o dowolnych podstawach (graniastosłupy, ostrosłupy, ostrosłupy ścięte, kula, stożek oraz walec), w tym: • automatyczne rysowanie graniastosłupów o dowolnej podstawie np.: podstawie trójkąta, kwadratu, czy dowolnego zadanego wielokąta foremnego • automatyczne rysowanie dowolnego ostrosłupa np. ostrosłupa o podstawie trójkąta, kwadratu, czy dowolnego zadanego wielokąta foremnego • automatyczne rysowanie dowolnego ostrosłupa ściętego np. ostrosłupa o podstawie trójkąta, kwadratu, czy dowolnego zadanego wielokąta foremnego • automatyczne rysowanie sześcianu • automatyczne rysowanie czworościanu • automatyczne rysowanie walca • automatyczne rysowanie stożka • automatyczne rysowanie kuli • automatyczne rysowanie półkuli 23. Każda ww. figura przestrzenna powinna dawać możliwość zmiany koloru i grubości linii, kolorowanie podstaw i ścian bocznych wraz ze efektem przezroczystości oraz wprowadzania faktury minimum 50 wzorów, rysowania tzw linii niewidocznych wewnątrz figur przestrzennych wraz z nadaniem im dowolnego koloru oraz różnych wzorów. 24. Każda przestrzenna figura jak sześcian, czworościan, stożek, prostopadłościan, ostrosłup, ostrosłup ścięty czy stożek ścięty muszą mieć możliwość przekręcania (obrotu) o zadany kąt oraz płynnie o dowolny. 25. Musi umożliwiać automatyczne wykreślanie osi współrzędnych XY 26. Musi umożliwiać nanoszenie na układ XY dowolnego wykresu funkcji o zadanym wzorze matematycznym postaci y=f(x) 27. Musi posiadać bibliotekę podstawowych wzorów i wykresów matematycznych, prostych z aktywnymi wzorami ax+by+c=0, paraboli z aktywnymi wzorami y=ax2+bx+c, x=ay2+by+c, (x-h)2=2p(y-k), (y-k)2=2p(x-k)), hiperboli (z aktywnymi wzorami), elips z aktywnymi wzorami, sinus z aktywnymi wzorami, cosinus z aktywnymi wzorami, tangens z aktywnymi wzorami, cotangens z aktywnymi wzorami, funkcje logarytmiczne z aktywnymi wzorami, dowolne funkcje kołowe z aktywnymi wzorami itp.. tak aby w jak najdokładniejszy sposób można było nie tylko wykreślić dowolną funkcję w układzie współrzędnych XY ale również pokazać jak się ona zachowuje podczas zmiany jej parametrów. 28. Musi umożliwiać poprawienie dowolnego ww. wykresu poprzez zmianę parametrów 29. Musi umożliwiać wprowadzanie parametrów danej funkcji w postaci funkcji kanonicznej oraz parametrycznej 30. Musi umożliwiać wrysowywanie 2 płaszczyzn z możliwością zmiany kąta pomiędzy tymi płaszczyznami 31. Musi posiadać alfabet grecki do zapisów matematycznych 32. Musi umożliwiać przygotowywanie dowolnego „doświadczenia chemicznego” na tablicy 33. Musi posiadać bibliotekę skalowalnych naczyń i przyborów laboratoryjnych z opcją dowolnego kolorowania, ustalania poziomu płynu oraz wypełniania dowolnym wzorem i kolorem płynów 34. Musi posiadać bibliotekę minimum 20 podstawowych zestawów doświadczeń laboratoryjnych, w których nauczyciel może każdy składowy element dowolnie zakolorować i wypełnić dowolnym rodzajem i kolorem substancji 35. Musi posiadać wzory i schematy ułatwiające tworzenie wzorów i schematów związków chemii organicznej 36. Musi posiadać bibliotekę skalowalnych diagramów i schematów elementów elektrotechnicznych pozwalającą narysować dowolny schemat elektrotechniczny 37. Musi posiadać bibliotekę skalowalnych diagramów i schematów elementów mechanicznych pozwalająca narysować dowolny schemat mechaniczny 38. Musi posiadać otwartą dożywotnią licencję pozwalającą na instalację i korzystanie w danej szkole na dowolnej liczbie komputerów bez konieczności dokonywania jakiejkolwiek rejestracji. 39. Oprogramowanie dostarczone wraz z monitorem musi umożliwiać przygotowywanie nauczycielom i uczniom w domach lekcji lub prezentacji za pomocą tego oprogramowania bez dodatkowych licencji i bez ograniczenia czasowego. 40. Nie dopuszcza się łączenia programów od różnych producentów 41. Oprogramowanie musi działać i zawierać wszystkie wymienione funkcje bez

	konieczności podłączenia do Internetu. 42. Program powinien zawierać: • bezpośredni odnośnik do Wikipedii • interaktywny model komórki • interaktywną tablicę Mendelejewa • interaktywne szkło powiększające • interaktywny tłumacz • Interaktywny wykres XY z dowolnymi funkcjami • proste interaktywne gry; • proste doświadczenia fizyczne • interaktywne doświadczenia z wagą • interaktywne doświadczenia z kostkami do gr • interaktywna tablica do nauki tabliczki mnożenia do 100 • interaktywna gra matematyczna kółko i krzyżyk
Warunki gwarancji	5 lat;
Wymagania dodatkowe	System operacyjny, kabel HDMI i USB, czujnik światła otoczenia, slot OPS, pilot z bateriami, 2 pisaki, zgodność ze standardem VESA, uchwyt ścienny i montaż;

XVII. Oprogramowanie biurowe Typ II – 20 szt.

Kompletny pakiet oprogramowania biurowego musi spełniać następujące wymagania, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Wymagania odnośnie interfejsu użytkownika:
   a) Pełna polska wersja językowa interfejsu użytkownika;
   b) Prostota i intuicyjność obsługi, pozwalająca na prace osobom nieposiadającym umiejętności technicznych;
   c) Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej musi być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się;
2. Oprogramowanie musi umożliwiać tworzenie i edycje dokumentów elektronicznych w formacie, który spełnia następujące warunki:
   a) posiada kompletny i publicznie dostępny opis formatu,
   b) ma zdefiniowany układ informacji w postaci XML zgodnie z Tabela B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)
   c) umożliwia wykorzystanie schematów XML
   d) wspiera w swojej specyfikacji podpis elektroniczny zgodnie z Tabela A.1.1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)
3. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb użytkownika oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców;
4. W skład oprogramowania muszą wchodzić narzędzia umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami;
5. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim;.
6. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
   a) Edytor tekstów
   b) Arkusz kalkulacyjny
   c) Narzędzie do przygotowywania i prowadzenia prezentacji/ tworzenia, edytowania i wyświetlania prezentacji
   d) Narzędzie do zarzadzania informacja prywatną (poczta elektroniczna, kalendarzem, kontaktami i zadaniami)
7. Edytor tekstu musi umożliwiać:
   a) Edycję i formatowanie tekstu w języku polskim wraz z obsługa języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty
   b) Wstawianie oraz formatowanie tabel
   c) Wstawianie oraz formatowanie obiektów graficznych
   d) Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne)
   e) Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków
   f) Automatyczne tworzenie spisów treści
   g) Formatowanie nagłówków i stopek stron
   h) Sprawdzanie pisowni w języku polskim
   i) Śledzenie zmian wprowadzonych przez użytkowników
   j) Nagrywanie, tworzenie i edycje makr automatyzujących wykonywanie czynności
   k) Określenie układu strony (pionowa/pozioma)
   l) Wydruk dokumentów
   m) Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarzadzania informacją prywatną
   n) Prace na posiadanych przez zamawiającego dokumentach utworzonych przy pomocy Microsoft Word 2010, 2013 i 2016 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu
   o) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji

p) Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostepniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem.
q) Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.
r) Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostepniającego formularze i pozwalające zapisać plik wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i Prawnych.

8. Arkusz kalkulacyjny musi umożliwiać:
   a) Tworzenie raportów tabelarycznych
   b) Tworzenie wykresów liniowych (wraz linia trendu), słupkowych, kołowych
   c) Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
   d) Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)
   e) Obsługę kostek OLAP oraz tworzenie i edycje kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiazywanie problemów optymalizacyjnych
   f) Tworzenie raportów tabeli przestawnych umożliwiających dynamiczna zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych
   g) Wyszukiwanie i zamianę danych
   h) Wykonywanie analiz danych przy użyciu formatowania warunkowego
   i) Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
   j) Nagrywanie, tworzenie i edycje makr automatyzujących wykonywanie czynności
   k) Formatowanie czasu, daty i wartości finansowych z polskim formatem
   l) Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
   m) Zachowanie pełnej zgodności z formatami posiadanych przez zamawiającego plików utworzonych za pomocą oprogramowania Microsoft Excel 2010, 2013 i 2016 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń..
   n) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
9. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać przygotowywanie prezentacji multimedialnych oraz:
   a) Prezentowanie przy użyciu projektora multimedialnego
   b) Drukowanie w formacie umożliwiającym robienie notatek
   c) Zapisanie w postaci tylko do odczytu.
   d) Nagrywanie narracji dołączanej do prezentacji
   e) Opatrywanie slajdów notatkami dla prezentera
   f) Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
   g) Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
   h) Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
   i) Tworzenie animacji obiektów i całych slajdów
   j) Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera
   k) Pełna zgodność z formatami plików posiadanych przez zamawiającego, utworzonych za pomocą oprogramowania MS PowerPoint 2010, 2013 i 2016.
10. Narzędzie do zarzadzania informacja prywatna (poczta elektroniczna, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
   a) Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego
   b) Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców
   c) Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną
   d) Automatyczne grupowanie poczty o tym samym tytule
   e) Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczna do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy
   f) Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia
   g) Zarzadzanie kalendarzem
   h) Udostępnianie kalendarza innym użytkownikom
   i) Przeglądanie kalendarza innych użytkowników
   j) Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach
   k) Zarzadzanie lista zadań
   l) Zlecanie zadań innym użytkownikom
   m) Zarzadzanie listą kontaktów
   n) Udostępnianie listy kontaktów innym użytkownikom
   o) Przeglądanie listy kontaktów innych użytkowników
   b) Możliwość przesyłania kontaktów innym użytkowników
11. Licencja edukacyjna, niewygasająca. Nie dopuszcza się licencji w modelu subskrypcyjnym;

XVIII. Laptopy – 2 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, aplikacji graficznych, dostępu do internetu oraz poczty elektronicznej
Ekran	15.6 FHD, IPS lub VA, 1920 x 1080, powłokąaprzeciwodblaskowa, jasność 220 nits
Wydajność	Oferowany komputer musi osiągać w teście wydajności BAPCO Sysmark 25 wynik 1000 pktWymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.).
Pamięć RAM	16 GB z możliwością rozbudowy do 32 GB RAM.
Pamięć masowa	256GB NVMe SSD M.2
Grafika	Posiadająca wsparcie do DirectX 12.
Klawiatura	Klawiatura odporna na zalanie, układ US, 100 klawiszy. Wszystkie klawisze funkcyjne typu: mute, regulacja głośności, print screen dostępne w ciągu klawiszy F1-F12.
Multimedia	Karta dźwiękowa zintegrowana z płytą główną; Wbudowane dwa głośniki stereo 2x2W. Cyfrowy mikrofon z funkcją redukcji szumów i poprawy mowy wbudowany w obudowę matrycy. Kamera internetowa 720p z diodą informującą o aktywności, trwale zainstalowana w obudowie matrycy. 1 port audio typu combo (słuchawki i mikrofon)
Łączność bezprzewodowa	Wi-Fi 5 ax 2x2 + Bluetooth 5
Bateria i zasilanie	35Whr. umożliwiająca szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin. Czas pracy na baterii - 7 godzin, potwierdzony wynikiem testu MobileMark25 Battery Life - **do oferty załączyć wynik testu testu lub link do publikacji na stronie BAPCO, w oferowanej konfiguracji**; Zasilacz o mocy 65W;
Waga i wymiary	Maksymalnie 2 kg. z baterią
Obudowa	Szkielet obudowy i zawiasy notebooka wzmacniane; Dookoła matrycy uszczelnienie chroniące klawiaturę po zamknięciu przed kurzem i wilgocią.
Certyfikaty	Laptop musi być wyprodukowany zgodnie z normami ISO9001 i ISO50001 ~~**– certyfikaty załączyć do oferty;**~~
Diagnostyka	System diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub z poziomu menu boot, umożliwiający przetestowanie komponentów komputera. Pełna funkcjonalność systemu diagnostycznego musi być realizowana bez: dostępu do sieci i internetu, dysku twardego również w przypadku jego braku, urządzeń zewnętrznych i wewnętrznych typu : pamięć flash, pendrive;
Bezpieczeństwo	TPM;
Porty i złącza	Wbudowane (nie dopuszcza się przejściówek): 1 x HDMI 1.4 1 x RJ-45, 3 x USB w tym 2 x USB 3.2, port zasilania, złącze linki zabezpieczającej
Warunki gwarancyjne	Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. 3-letnia gwarancja, czas reakcji serwisu, do końca następnego dnia roboczego. Oferent musi posiadać ISO 9001 i ISO27001 na serwis rozwiązań informatycznych ~~**– certyfikat załączyć do oferty**~~
System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w języku polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i

	przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z poziomów: menu, otwartego okna systemu operacyjnego; 7. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 8. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 9. Graficzne środowisko instalacji i konfiguracji w języku polskim 10. Wbudowany system pomocy w języku polskim. 11. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 12. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora Zamawiającego. 13. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 14. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, w tym możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 15. Zabezpieczony hasłem hierarchiczny dostęp do systemu; 16. Konta i profile użytkowników zarządzane zdalnie; 17. Praca systemu w trybie ochrony kont użytkowników. 18. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze; 19. Molliwość zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 20. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na serwerze plików z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika 21. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 22. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 23. Oprogramowanie dla tworzenia kopii zapasowych (Backup); 24. Automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 25. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 26. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 27. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu); 28. Wbudowany mechanizm wirtualizacji typu hypervisor; 29. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem interfejsu graficznego. 30. Bezpłatne biuletyny bezpieczeństwa związane z działaniem systemu operacyjnego. 31. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; 32. Zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 33. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny; 34. Zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej i udostępnianiem plików; 35. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. 36. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi i niezarządzanymi. 37. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne; 38. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 39. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych; 40. Możliwość tworzenia wirtualnych kart inteligentnych. 41. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 42. Wsparcie dla IPSEC oparte na politykach; 43. Wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; 44. Mechanizmy logowania w oparciu o: a) Login i hasło, b) Karty inteligentne i certyfikaty (smartcard), c) Wirtualne karty inteligentne i certyfikaty chronione poprzez moduł TPM; 45. Umozliwiajacy pracę w domenie;
Oprogramowanie	System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV

użytkowe	Comperative Advance + musi umożliwiać co najmniej: 1. Wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji, 2. Wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych, 3. Stosowanie kwarantanny 4. Wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear) 5. Skanowanie urządzeń USB natychmiast po podłączeniu, 6. Automatyczne odłączanie zainfekowanej końcówki od sieci, 7. Skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji. 8. Zarządzanie stacją kliencką poprzez zbieranie informacji co najmniej o: nazwie, producencie i modelu komputera, przynależności do grupy roboczej/domeny, szczegółach systemu operacyjnego, lokalnych kontach użytkowników, dacie i godzinie uruchomienia i ostatniego restartu komputera, parametrach sprzętowych (procesor, RAM, SN, dysk), BIOS, interfejsach sieciowych, dołączonych peryferiach. 9. Musi posiadać moduł ochrony IDS/IPS 10. Musi posiadać mechanizm wykrywania skanowania portów 11. Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów 12. Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości 13. Oprogramowanie do szyfrowania, chroniące dane na stacji za pomocą algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. 14. Pełne szyfrowanie dysków działających w oferowanych komputerach zapobiegające utracie danych z powodu utraty / kradzieży stacji roboczej. 15. Oprogramowanie musi szyfrować całą zawartość na urządzeniach przenośnych, takich jak pendrive, dyski USB i udostępniać ją tylko autoryzowanym użytkownikom. 16. Musi umożliwiać blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji; 17. Musi umożliwiać zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji. 18. Możliwość blokady zapisywania plików na zewnętrznych dyskach USB oraz możliwości uruchamiania oprogramowania z takich dysków. Blokada ta musi umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach. 19. Interfejs zarządzania musi wyświetlać monity o zbliżającym się zakończeniu licencji, a także powiadamiać o zakończeniu licencji. 20. Moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware poprzez ograniczenie możliwości modyfikowania chronionych plików, tylko do procesów systemowych oraz zaufanych aplikacji. 21. Możliwość zdefiniowania chronionych folderów zawierających wrażliwe dane użytkownika. 22. Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych ochroną any ransomware. 23. Monitorowanie krytycznych danych użytkownika zapobiegające atakom ransomware; 24. Centralna konsola zarządzająca umożliwiająca co najmniej: a) przechowywanie danych w bazie typu SQ b) zdalną instalację lub deinstalację oprogramowania, na pojedynczych stacjach, zakresie adresów IP lub grupie z ActiveDirectory; c) tworzenie paczek instalacyjnych oprogramowania, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi oraz formatach dla systemów Linux d) centralną dystrybucję uaktualnień definicji ochronnych, których źródłem będzie plik na serwerz konsoli; e) raportowanie z prezentacją tabelaryczną i graficzną, możliwością automatycznego czyszczenia starych raportów, eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich; f) definiowanie struktury opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji; 25. Możliwość tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera; 26. Dostęp do konsoli z dowolnego miejsca w nagłych przypadkach; 27. Możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń 28. Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach. 29. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych; 30. System musi umożliwiać, z konsoli na serwerze, co najmniej:

	a) różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie b) przyznawanie praw dostępu dla nośników pamięci tj. USB, CD c) regulowania połączeń WiFi i Bluetooth d) kontrolowanie i regulowanie użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe e) blokadę lub zezwolenia na połączenie się z urządzeniami mobilnymi f) blokowanie dostępu dowolnemu urządzeniu g) tymczasowe dodanie dostępu do urządzenia przez administratora h) szyfrowanie zawartości USB i udostępnianie jej na stacjach końcowych; i) zablokowanie funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszk j) zezwalanić na dostęp tylko urządzeniom wcześniej dodanym przez administratora k) używanda tylko zaufanych urządzeń sieciowych; 31. Funkcja wirtualnej klawiatury 32. Możliwość blokowania każdej aplikacji , w tym w oparciu o kategorie 33. Możliwość dodania własnych aplikacji do listy zablokowanych 34. Tworzenie listy aplikacji zainstalowanych na komputerach klientach poprzez konsolę administracyjną na serwerze 35. Kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool 36. Możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki; 37. Możliwość zablokowania funkcji Printscreen 38. Monitorowanie przesyłu danych między aplikacjami; 39. Monitorowanie i kontrola przepływu poufnych informacji 40. Blokowanie plików w oparciu o ich rozszerzenie lub rodzaj 41. Monitorowanie i zarządzanie danymi udostępnianymi poprzez zasoby sieciowe; 42. Ochrona przed wyciekiem informacji na drukarki lokalne i sieciowe 43. Ochrona zawartości schowka systemu 44. Ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL 45. Dodawanie wyjątków dla domen, aplikacji i lokalizacji sieciowych 46. Ochrona plików zamkniętych w archiwach 47. Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem 48. Możliwość tworzenia profilu DLP dla każdej polityki 49. Wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania 50. Ochrona przez wyciekiem plików poprzez programy typu p2p 51. Monitorowanie działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych. 52. Monitorowanie określonych rodzajów plików. 53. Możliwość wykluczenia określonych plików/folderów z procedury monitorowania. 54. Możliwość śledzenia zmian we wszystkich plikach 55. Możliwość śledzenia zmian w oprogramowaniu zainstalowanym na stacjach roboczych; 56. Możliwość definiowana własnych typów plików 57. Usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku 58. Optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem 59. Możliwość zaplanowania optymalizacji na wskazanych stacjach klienckich 60. System ochrony i zarządzania urządzeniami za pomocą platformy w chmurze;. 61. Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi 62. Musi posiadać możliwość eksportu danych użytkownika 63. Import listy urządzeń z pliku CSV 64. Dodawanie urządzeń; 65. Podgląd co najmniej następujących informacji konfiguracji: data i status wdrożenia, status urządzenia, numer telefonu, właściciel, grupa, reguły, wersja agenta 66. Podgląd co najmniej następujących informacji sprzętowych: model, producent, system, adres MAC, bluetooth, wolna przestrzeń na dysku, całkowita przeszłość na dysku, użycie procesora,; 67. Podgląd zainstalowanych aplikacji; 68. Moduł raportowania aktywności, skanowania oraz naruszenia reguł; 69. Oprogramowanie pozwalające na wykrywanie oraz zarządzanie podatnościami bezpieczeństwa dostępne przez przeglądarkę internetową; 70. Portal zarządzający w postaci SaaS; 71. Skanowanie podatności za pomocą nodów skanujących; 72. Nody skanujące w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie 73. Portal zarządzający musi umożliwiać: a) przegląd wybranych danych; b) zablokowanie możliwości zmiany konfiguracji; c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów;

	d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności e) eksport skanów podatności do pliku CSV; 74. **D**eduplikacja danych na źródle, 75. Backup przyrostowy i różnicowy, 76. Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji, 77. Backup danych lokalnych – plikowy oraz poczty; 78. Backup otwartych plików; 79. Filtr plików oraz folderów, 80. Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.), 81. Przywracanie danych do wskazanej lokalizacji, 82. Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora, 83. Wyszukiwanie plików w repozytorium użytkownika, 84. Automatyczne logowanie, 85. Zapamiętywanie danych logowania, 86. Automatyczne uruchamianie programu przy starcie systemu, 87. Ustawianie priorytetu dla procesu backupu, 88. Zmiana klucza szyfrującego, 89. Konfiguracja wydajności procesu backupu, 90. Zastępowanie nazwy pliku GUID-em, 91. Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika, 92. Kompresja danych, 93. Transmisja po bezpiecznym protokole TLS, 94. Deklaracja klucza szyfrującego dane użytkownika, 95. Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji, 96. Obliczanie sumy kontrolnej, 97. Kopie zapasowe musza być przechowywane w data center, na terenie Polski. 98. Licencje muszą być przypisywane do urządzenia z limitem pojemności przestrzeni w chmurze minimum 50 GB; 99. Wsparcie techniczne, świadczone w języku polskim;

XVIII. Oprogramowanie antywirusowe – 3 kpl.

I. Zamawiajacy wymaga dostarczenia 3 kompletów licencji w następujących konfiguracjach:
   a) Serwer + 7 stacji
   b) Serwer + 14 stacji
   c) Serwer + 8 stacji

II. Subskrypcje na 36 m-c;

III. Oprogramowanie musi spełniać następujące wymagania:

1. Wsparcie dla posiadanych przez zamawiającego systemów Windows: 10, 8,7.
2. Wsparcie dla posiadanych przez zamawiającego systemów: Windows Server: 2019, 2016, 2012 R2;
3. Interfejsy programu, pomoce i podręczniki w języku polskim.
4. Ochrona przed zagrożeniami typu 0-day na poziomie co najmniej 97%;
5. Ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
6. Wykrywanie i usuwanie niebezpiecznych programów: adware, spyware, scareware, phishing, hacktools;
7. Wbudowana technologia do ochrony przed rootkitami wykrywająca aktywne i nieaktywne rootkity.
8. Moduł do ochrony przed exploitami (ataki 0-day).
9. Moduł do ochrony przed ransomware.
10. Mechanizm ochrony przed zamaskowanym złośliwym kodem wykorzystujący sieć neuronową opartą o algorytmy adaptacyjne;
11. Klient oprogramowania antywirusowego dla stacji roboczych z systemami Linux.
12. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
13. Dwa niezależne skanery antywirusowe z dwoma niezależnymi bazami sygnatur wirusów wykorzystywane przez skaner dostępowy, skaner na żądanie oraz skaner poczty elektronicznej.
14. Możliwość konfiguracji programu do pracy z jednym skanerem i dwoma skanerami antywirusowymi jednocześnie.
15. Niezależny od skanerów plików, trzeci skaner poczty oparty o technologię cloud security.
16. Możliwość wykluczenia ze skanowania skanera dostępowego: napędów, katalogów, plików lub procesów.
17. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików na żądanie lub według harmonogramu.
18. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu;
19. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rodzaj plików do skanowania, priorytet skanowania);
20. Skanowanie na żądanie pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
21. Technologia zapobiegająca powtórnemu skanowaniu sprawdzonych już plików, przy czym maksymalny czas od ostatniego sprawdzenia pliku nie może być dłuższy niż 4 tygodnie, niezależnie od tego czy plik był modyfikowany czy nie.
22. Możliwość określania poziomu obciążenia procesora podczas skanowania na żądanie i według harmonogramu;
23. Możliwość skanowania dysków sieciowych i dysków przenośnych.
24. Rozpoznawanie i skanowanie wszystkich znanych formatów kompresji.

25. Możliwość definiowania listy procesów, plików, folderów i napędów pomijanych przez skaner dostępowy.
26. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (kwarantanna) w celu dalszej kontroli.
27. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
28. Skanowanie i oczyszczanie poczty przychodzącej POP3 w czasie rzeczywistym, zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej;
29. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
30. Możliwość definiowania różnych portów dla POP3, SMTP i IMAP na których ma odbywać się skanowanie.
31. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odebranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
32. Dodatek umożliwiający podejmowanie działań związanych z ochroną z poziomu programu pocztowego.
33. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch musi być automatycznie blokowany a użytkownikowi wyświetlane musi być powiadomienie;
34. Dedykowany moduł chroniący przeglądarki przed szkodnikami atakującymi sesje z bankami i sklepami online.
35. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
36. Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie.
37. Ochrona przed stronami phishingowymi działającymi przy użyciu protokołów HTTP i HTTPS.
38. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
39. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń muszą być w pełni anonimowe.
40. Możliwość automatycznego wysyłania powiadomienia o wykrytych zagrożeniach do dowolnej stacji roboczej w sieci lokalnej.
41. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e mail.
42. Możliwość zabezpieczenia hasłem dostępu do opcji konfiguracyjnych programu.
43. Aktualizacja dostępna z bezpośrednio Internetu lub offline – z pliku pobranego zewnętrznie.
44. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
45. Możliwość określenia częstotliwości aktualizacji w odstępach 1 godzinowych.
46. Możliwość samodzielnej aktualizacji sygnatur wirusów ze stacji roboczej;
47. Program wyposażony w jeden serwer skanujący uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, skaner HTTP).
48. Możliwość ukrycia programu na stacji roboczej przed użytkownikiem.
49. Moduł ochrony proaktywnej, uczący się zachowania systemu operacyjnego i wykrywający podejrzane działania.
50. Skanowanie w trybie bezczynności - pełne skanowanie komputera przynajmniej raz na 2 tygodnie uruchamiane i wznawiane automatycznie, podczas gdy nie jest on używany
51. Ochrona przed urządzeniami podszywającymi się pod klawiatury USB.
52. Agentowa ochrona maszyn wirtualnych wykrywająca znane i nieznane zagrożenia przy użyciu zdalnego serwera skanowania oraz technologii proaktywnych.
53. Agent ochrony maszyn wirtualnych delegujący zlecenie skanowania do wirtualnego serwera skanowania.
54. Wirtualny serwer skanowania dostarczony w formie gotowego obrazu dla środowisk HyperV oraz VMware;
55. Integracja z posiadana przez zamawiającego usługą Active Directory, w tym co najmniej import kont komputerów i jednostek organizacyjnych.
56. Ochrona dla posiadanych przez zamawiającego urządzeń z systemem Android i iOS.
57. Konsola administracyjna pobierająca interfejs zgodny z serwerem zarządzającym.
58. Automatyczna instalacja oprogramowania klienckiego na wszystkich podłączonych komputerach Active Directory.
59. Zdalna instalacja i centralne zarządzanie klientami na stacjach roboczych i serwerach;
60. Do instalacji zdalnej i zarządzania zdalnego nie może być wymagany dodatkowy agent. Na końcówkach zainstalowany musi być sam program antywirusowy.
61. Możliwość zarządzania ochroną urządzeń mobilnych z poziomu konsoli (co najmniej: aktualizacje, ochronę przeglądarek, skanowania zasobów, synchronizacji raportów).
62. Możliwość kontekstowego zastosowania ustawień danej stacji dla całej grupy.
63. Możliwość eksportu/importu ustawień dla stacji/grupy stacji.
64. Możliwość zarządzania dowolną ilością serwerów zarządzających z jednego okna konsoli.
65. Możliwość zarządzania różnymi wersjami licencyjnymi oprogramowania producenta z jednego okna konsoli.
66. Możliwość tworzenia hierarchicznej struktury serwerów zarządzających (serwer główny i serwery podrzędne).
67. Możliwość zainstalowania zapasowego serwera zarządzającego, przejmującego automatycznie funkcje serwera głównego w przypadku awarii lub odłączenia serwera głównego.
68. Możliwość zdalnego zarządzania serwerem spoza sieci lokalnej przy pomocy połączenia VPN.
69. Możliwość zarządzania ochroną wielu sieci z poziomu jednej instancji serwera zarządzającego.
70. Szyfrowanie komunikacji między serwerem zarządzającym a klientami.
71. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.
72. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (co najmniej: aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania).
73. Możliwość przeglądania list programów zainstalowanych na stacjach/serwerach (co najmniej: nazwa, wersja, producent, data instalacji).
74. Możliwość stworzenia białej i czarnej listy oprogramowania, i późniejsze filtrowanie;
75. Odczyt informacji o zasobach sprzętowych stacji (procesor i jego taktowanie, ilość pamięci RAM i ilość miejsca na dysku/partycji systemowej).
76. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu

77. Możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych.
78. Możliwość tworzenia grup stacji roboczych i definiowania w ramach grupy wspólnych ustawień konfiguracyjnymi dla zarządzanych programów.
79. Możliwość zmiany konfiguracji na stacjach i serwerach z centralnej konsoli zarządzającej lub lokalnie;
80. Możliwość generowania raportów w formacie XML.
81. Możliwość przeglądania statystyk ochrony antywirusowej w postaci tekstu lub wykresów.
82. Możliwość przesłania komunikatu, który wyświetli się na ekranie wybranej stacji roboczej lub grupie stacji roboczych.
83. Możliwość zminimalizowania obciążenia serwera poprzez ograniczenie ilości jednoczesnych procesów synchronizacji, aktualizacji i przesyłania plików do stacji roboczych.
84. Możliwość grupowania stacji na podstawie parametrów: nazwa komputera, adres IP, brama domyślna, nazwa domeny.
85. Możliwość utworzenia raportów statusu ochrony sieci.
86. Możliwość wysyłania raportów z określonym interwałem.
87. Możliwość wysłania jednego raportu na różne adresy mailowe lub grupy adresów.
88. Zdalna instalacja, zdalne zarządzanie wszystkimi funkcjami zapory i zdalna deinstalacja.
89. Zapora działająca domyślnie trybie automatycznego rozpoznawania niegroźnych połączeń i tworzenia reguł bez udziału użytkownika.
90. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.
91. Możliwość interakcji między użytkownikiem a administratorem w celu dostosowania zestawu reguł.
92. Możliwość zdefiniowania osobnych zestawów reguł dla dowolnych grup użytkowników.
93. Wbudowany system IDS.
94. Możliwość pracy w trybie offsite po odłączeniu od sieci przedsiębiorstwa.
95. Wykrywanie zmian w aplikacjach korzystających z sieci na podstawie sum kontrolnych i monitorowanie o tym zdarzeniu.
96. Możliwość automatycznego skanowania antywirusowego modułów o zmodyfikowanych sumach kontrolnych.
97. Automatyczne wysyłanie powiadomień o zablokowaniu aktywności sieciowej na wskazany adres mailowy.
98. Import/eksport reguł/zestawów reguł zapory na stacji roboczej;

XIX. Serwer NAS – 4 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Procesor	Musi osiagać wynik 700 wteście PassMark CPU Mark
Pamięć	2 GB ;
Pamięc flash	4 GB;
Zatoki na dyski	2 szt.;
Obsługiwane dyski	2,5 cala SSD SATA oraz 3,5 cala SATA; hot swap;
Porty	1 z GbE; 3 x USB;
Obudowa	Tower lub rack
Diody	LAN, USB, zatoki dyskowe;
Zasilacz	65W;
Wentylator	1 x 80 mm;
CIFS	200;
Rozmiar puli	300 TB;
Ilość pul	128
Zainstalowane dyski	2 x 2 TB SATA 6 Gb/s; MTBF – 1 mln. godzin, Pamięc podręczna – 128 MB; Szybkość transferu – 140 MB/s.; Obciążalność – 180 TB/rok; Gwarancja – 3 lata; Głośność podczas pracy – maksymalnie 25 dBA; Pobór mocy podczas pracy – maksymalnie 5 W;
Pobór mocy podczas pracy	Maksymalnie 15W;
System operacyjny	1. Pula pamieci SED; 2. Obsługiwany rozmiar woluminu – 250 TB; 3. Liczba folderów udostpenianych – 512; 4. Rozmiar folderu udostępnianego – 250 TB; 5. Rozszerzenie JBOD;

	6. VJBOD; 7. Usługa iSCSI i FC; 8. Jednostka iSCSI LUN oparta na plikach i blokach; 9. Funkcje LUN: 10. Mapowanie LUN; 11. Przenoszenie jednostki LUN między iSCSI i FC; 12. Maskowanie LUN 13. Import/eksport aliasów WWPN 14. Wiązanie portu FC 15. Wielościeżkowe we/wy (MPIO) 16. Rozszerzenie pojemności jednostek LUN online 17. Migawka jednostki LUN 18. Replikacja migawek jednostek LUN i klonowanie; 19. Automatyczne wartswowanie; 20. Obsługa RAID - JBOD, RAID 0, 1; 21. Migracja RAID; 22. Rozszerzenie RAID i puli pamięci; 23. Hot spare RAID; 24. Szacowanie żywotności dysków SSD; 25. Migawka jednostki LUN; 26. 64 migawki na urządzenie i 32 na jednostkę LUN; 27. Interwał migawki – 5 minut; 28. Samoobsługowe odzyskiwanie migawek; 29. Migawka złożona z aplikacji; 30. Pamięć podręczna do odczytu i zapisu; 31. Narzędzie do profilowania SSD; 32. Zarządzanie zewnętrznym urządzeniem RAID; 33. Serwer plików; 34. Serwer FTP; 35. Kontroler domeny; 36. Limitowanie liczby użytkowników; 37. Monitor zasobów; 38. SNMP v2 i 3 39. Odzyskiwanie plików usuniętych ; 40. Automatyczne czyszczenie i filtr typu pliku 41. Dziennik systemowy i centrum powiadomień; 42. Harmonogram włączania i wyłaczania; 43. Przełącznik wirtualny; 44. Trunkowanie portów; 45. Serwer DHCP;
Gwarancja	2 lata;

XX. UTM – 3 szt.

1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP;
2. Urządzenie musi być wyposażone w Firewall klasy Stateful Inspection.
3. Urządzenie musi obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
4. Urządzenie musi umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
5. Interface (GUI) do konfiguracji firewall musi umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów.
6. Osoba administrująca musi mieć możliwość określania parametrów pojedynczej reguły przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
7. Administrator musi mieć możliwość:
   a) budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, użytkownika bądź grupy z bazy LDAP,;
   b) określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
8. Urządzenie musi umożliwiać filtrowanie jedynie na poziomie warstwy 2 na podstawie adresów mac.
9. Administrator muai mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
10. Edytor reguł firewall musi posiadać wbudowany analizator, który wskazuje błędy i sprzeczności w konfiguracji reguł.
11. Urządzenie musi umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP, zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
12. Urządzenie musi umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routing;).
13. System detekcji i prewencji włamań (IPS) musi być zaimplementowany w jądrze systemu i wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe;

14. Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy;.
15. Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
16. Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
17. Moduł IPS musi wykrywać i usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
18. Urządzenie musi umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.
19. Administrator musi mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP, użytkowników, portów;
20. Urządzenie musi umożliwiać ochronę przed atakami typu SQL Injection, Cross Site Scripting oraz złośliwym kodem Web2.0.
21. Urządzenie musi umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
22. Ograniczenie pasma lub priorytetyzacja reguły firewall musi być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika;
23. Urządzenie musi umożliwiać tworzenie kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu;
24. Urządzenie musi umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
25. Urządzenie musi umożliwiać zastosowanie skanera dostaronego przez firmę trzecią;
26. Administrator musi mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
27. Administrator musi mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP.
28. W przypadku SMTP i FTP musi być możliwość zdefiniowania kodu wykrycia infekcji.
29. Urządzenie musi posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
30. Ochrona antyspam musi działać w oparciu o:
    a. białe/czarne listy,
    b. DNS RBL,
    c. Skaner heurystyczny.
31. W przypadku ochrony w oparciu o DNS RBL administrator musi mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
32. Urządzenie musi umożliwiać stworzenie sieci VPN typu client-to-site lub site-to-site;
33. Urządzenie musi wspierać co najmniej następujące typy sieci VPN:
    a. PPTP VPN,
    b. IPSec VPN,
    c. SSL VPN.
34. SSL VPN musi działać co najmniej w trybach tunelu i portalu.
35. Producent urządzenia musi umożliwiać pobranie klienta VPN współpracującego z urządzeniem;
36. Urządzenie musi umożliwiać przełączenie tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
37. Urządzenie musi umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
38. Urządzenie musi posiadać wbudowany filtr URL.
39. Filtr URL musi działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
40. Administrator musi mieć możliwość dodawania własnych kategorii URL.
41. Administrator musi mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru musi być przynajmniej:
    a. blokowanie dostępu do adresu URL,
    b. zezwolenie na dostęp do adresu URL,
    c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
42. Administrator musi mieć możliwość skonfigurowania różnych stron z komunikatem o zablokowaniu strony.
43. Strona blokady muszą umożliwiać wykorzystanie zmiennych środowiskowych.
44. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
45. Urządzenie musi umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
46. Urządzenie musi umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
47. Urządzenie musi umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
    a. lokalną bazę użytkowników (wewnętrzny LDAP),
    b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
    c. usługę katalogową Microsoft Active Directory.
48. Urządzenie musi umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
49. Urządzenie musi umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
    a. SSL,
    b. Radius,
    c. Kerberos.
50. Urządzenie musi umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Active Directory;
51. Metoda transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
52. Autoryzacja użytkowników z Active Directory nie może wymagać modyfikacji schematu domeny.

53. Urządzenie musi umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
54. Mechanizm równoważenia obciążenia łącza internetowego musi działać w oparciu o następujące mechanizmy:
    a. równoważenie względem adresu źródłowego,
    b. równoważenie względem połączenia.
55. Mechanizm równoważenia obciążenia musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
56. Urządzenie musi umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (Failover).
57. Urządzenie musi wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
58. W zakresie SD-WAN urządzenie musi zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
59. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
60. Urządzenie musi umożliwiać statyczne trasowanie pakietów.
61. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
62. Urządzenie musi umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (Policy Based Routing).
63. Urządzenie musi umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
64. Konfiguracja urządzenia z wykorzystaniem polskiego interfejsu graficznego.
65. Interfejs konfiguracyjny dostępny poprzez przeglądarkę internetową, a komunikacja zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
66. Administrator musi mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
67. Urządzenie musi umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi uprawnieniami.
68. Urządzenie musi umożliwiać zarządzenia z poziomu konsoli (SSH)
69. Urządzenie musi umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
70. Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
71. Urządzenie musi umożliwiać zapisywanie logów na wbudowanym dysku.
72. Urządzenie musi umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
73. Urządzenie musi umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
74. Urządzenie musi umożliwiać eksportowanie backupu konfiguracji co najmniej w zakresie:
    a. manualnego eksportu do pliku w dowolnym momencie czasu,
    b. automatycznego eksportu do chmury producenta lub na dedykowany serwer zarządzany, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu
75. Urządzenie musi umożliwiać odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera;
76. Urządzenie musi umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
77. Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
78. System raportowania i przeglądania logów wbudowaey w system nie mogą wymagać dodatkowej licencji do swojego działania.
79. System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera antywirusowego, skanera antyspamowego.
80. System raportowania musi umożliwiać wygenerowanie co najmniej 25 różnych raportów.
81. System raportowania musi umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
82. W ramach posiadanej licencji urządzenie musi umożliwiać skorzystanie z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny.
83. Urządzenie musi umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
84. Urządzenie musi umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH)
85. Urządzenie musi posiadać wbudowany serwer DHCP z możliwością dynamicznego i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
86. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP;
87. Konfiguracja serwera DHCP musi być niezależna dla IPv4 i IPv6.
88. Urządzenie musi umożliwiać stworzenie różnych konfiguracji DHCP dla różnych podsieci w zakresie określenia bramy, serwerów DNS, nazwy domeny.
89. Urządzenie musi posiadać usługę DNS Proxy.
90. Urządzenie musi posiadać dwie niezależne partycje w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania firmware;
91. Możliwość zsynchronizowaniea aktywnej partycji z zapasową;
92. Urządzenie musi być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
93. W okresie obowiązywania gwarancji musi być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
94. Urządzenie musi być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
95. Urządzenie musi umożliwiać podłączenie karty SD w celu zapisywania logów.

96. 8 portów Ethernet 10/100/1000Mbps;
97. Urządzenie musi umożliwiać dostęp do internetu za pomocą modemu 3G oraz 4G;
98. Przepustowość Firewall (1518 bajtów UDP) –4Gbps.
99. Przepustowość Firewall wraz z włączonym systemem IPS – 2.4Gbps.
100. Przepustowość filtrowania Antywirusowego – 490 Mbps.
101. Przepustowość tunelu VPN przy szyfrowaniu AES –600Mbps.
102. Maksymalna liczba tuneli VPN IPSec –100.
103. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) –20.
104. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) –50.
105. Obsługa interfejsów 802.11q (VLAN) –128
106. Liczba równoczesnych sesji – 300 000 i 18 000 nowych sesji/sekundę.
107. Urządzenie musi umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
108. Urządzenie nie może mieć limitu na liczbę użytkowników.
109. Liczba reguł filtrowania –8 192.
110. Liczba tras statycznego routingu –512.
111. Liczba tras dynamicznego routingu –1
112. 3-godzinne wdrożenie w sieci zamawiającego;
113. Zakres wdrożenia:
    a) Zmiana domyślnych haseł,
    b) Zmiana strefy czasowej i ustawienie poprawnej daty/godziny,
    c) Rejestracja urządzenia na stronie producenta,
    d) Aktualizacja oprogramowania;
    e) Konfiguracja profili bezpieczeństwa IPS;
    f) Konfiguracja 4 portów LAN/WAN;
    g) Konfiguracja QOS lub failover / load balancing'u;
    h) Konfiguracja 20 reguł bezpieczeństwa firewall;
    i) Konfiguracja 5 reguł NAT;
    j) Utworzenie do 30 obiektów,
    k) Konfiguracja SSL VPN Client To Site;
    l) Konfiguracja 1 tunelu VPN Site To Site;
    m) Konfiguracja urządzenia w trybie routera (NAT) lub w trybie transparentnym
    n) Konfiguracja połączenia z AD (integracja) lub utworzenie lokalnej bazy LDAP;

XXI. Zestaw do autentykacji – 46 kpl.

1. Musi zabezpieczać komputer przed dostępem niepowołanych osób;
2. System musi być chroniony przez długie i skomplikowane hasło, którego użytkownik nie musi wpisywać każdorazowo podczas logowania;
3. Możliwość stworzenia specjalnego pendrive'a, na którym hasło zostanie zapisane;
4. Podłączenie pendrive do komputera podczas logowania musi powodować automatyczne przyznanie dostępu;
5. Bez posiadania pendrive'a nie może być możliwości zalogowania do systemu;
6. Program musi obsługiwać wiele tokenów weryfikacyjnych róznych producentów oraz klucze Bluetooth, czytniki RFID czy Google Authenticator;
7. Możliwość zabezpieczenia komputera za pomocą smartfona z Androidem lub iOS;
8. Tworzenie tokena musi odbywać się z poziomu programu;
9. Możliwość wprowadzenia kodu PIN na etapie konfiguracji;
10. Trzykrotne, błędne wprowadzenie kodu PIN musi blokować dostęp;
11. Możliwość logowania do systemu za pomocą hasła;
12. Możliwość manualniego wpisania hasła i wygenerowania losowego ciągu znaków;
13. Zmienione dane dostępowe musza być automatycznie zapisane na kluczu USB, podpiętym do komputera;
14. Moliwość określenia zachowania systemu po odłączeniu skonfigurowanego klucza sprzętowego, wtym co najmniej: brak działań, zablokowanie komputera, wylogowanie użytkownika, wyłączenie urządzenia, przejście w stan hibernacji, przełączenie użytkownika, uruchomienie wskazanego skryptu;
15. Możliwość włączenia logowania wyłącznie za pomocą skonfigurowanego nośnika;
16. Program musi pozwalać określić użytkowników, dla których dana funkcja ma zostać aktywowana;
17. Możliwosc skonfigurowania logowania awaryjnego na wypadek zgubienia klucza;
18. Możliwość wpisania czterech różnych pytań i wskazania dozwolonej liczby prób, po przekroczeniu której zalogowanie nie będzie możliwe;
19. Możliwość definiowania reguł obsługujących kontrolę uwierzytelniania wieloczynnikowego;
20. Automatyczne wybieranie metody silnego uwierzytelniania dla uprzywilejowanych użytkowników;
21. Zdalny dostęp do pulpitu i jednoczynnikowe uwierzytelnianie podczas regularnego korzystania z komputera;
22. Obsługa decyzji dotyczących uwierzytelniania wieloczynnikowego z możliwością użycia wielu modalności 2FA;
23. Obsługa bramki SMS dla OTP opartej na 2FA;
24. Obsługa Amazon WorkSpaces i Azure VDI;
25. MFA dla zdalnych komputerów z urządzeniami Google Auth OTP lub Yubikey;
26. Token TOTP musi być używany przez 5 godzin i być ważny kilka razy w określonym czasie jednego dnia;

27. Możliwość wyłączenia MFA dla zablokowanych sesji zdalnego pulpitu uwierzytelnionych za pomocą MFA;
28. Wyświetlani kont użytkowników na ekranie logowania
29. Import etykiety RFID według pliku CVS;
30. Wymiana hasła z kartami RFID HID.
31. Obsługa czytnika kart inteligentnych dla kart MiFare 1K.
32. W stacjach roboczych z Active Directory system musi zapisywać zdarzenia 2FA w dzienniku zdarzeń systemu operacyjnego;
33. Obsługa dynamicznej decyzji MFA:
    a) przez członkostwo grupy Active Directory użytkownika każdej próby dostępu;
    b) przez filtrowanie adresów IP użytkownika zdalnego pulpitu;
34. Możliwość wyłączenia MFA dla zablokowanych sesji pulpitu zdalnego
35. Mozłiwość wyłączenia historii OTP dla wielokrotnego użycia;
36. Możliwość udostępnienia operatorom komputerów wygenerowanych kodów OTP;
37. Kody OTP musza być ważne dla wybranego czasu i dnia pracy;
38. Ustawienie limit czasu dla sesji logowania do pulpitu zdalnego;
39. Logowanie do systemu operacyjnego za pomocą kart RFID;
40. Import karty RFID według numeru UID za pomocą pliku CSV z listą użytkowników i UID karty każdego użytkownika;
41. Obsługa zasad odnawiania hasła;
42. Pendrive o pojemności 16 GB – 46 szt;
43. Podłaczączany do portu USB i zakrywany zatyczką;
44. Możliwość przypięcia zawieszki;
45. Prędkość odczytu - 20 MB/s i zapisu - 5 MB/s;