**Załącznik nr 1 do SWZ**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**na zadanie pn.:„Dostawa sprzętu IT i oprogramowania dla potrzeb Urzędu Gminy Brzeźnica i jednostek podległych w ramach projektu „Cyfrowa Gmina”**

**Część I – Dostawa sprzętu IT i oprogramowania**

- Komputer stacjonarny – 21 szt.

- Laptop – 7 szt.

- Serwer Typ I – 1 szt.

- Serwer Typ II – 1 szt.

- Urządzenie wielofunkcyjne – Typ I – 2 szt.

- Urządzenie wielofunkcyjne – Typ II – 1 szt.

- Zasilacz awaryjny Typ I – 1 szt.

- Zasilacz awaryjny Typ II – 1 szt.

- Oprogramowanie biurowe Typ I – 22 szt.

- Oprogramowanie bazodanowe – 1 szt.

- Oprogramowanie serwerowe – 1 szt.

- Tablet – 15 szt.

- System operacyjny – 24 szt.

1. **Komputer stacjonarny – 21 szt.**

|  |  |  |
| --- | --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | |
| Typ | Komputer stacjonarny. Typu All in One, komputer fabrycznie wbudowany w obudowę monitora. | |
| Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna | |
| Wydajność | Oferowany komputer musi osiągać w teście wydajności SYSMARK 25 Overall Rating, wynik 1150 pkt. **Wydruk z oprogramowania testującego załączyć do oferty.**  Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS ( tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.).  Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów Oferent musi dostarczyć Zamawiającemu oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego | |
| Pamięć RAM | 8GB DDR4 2666MHz. Możliwość rozbudowy do 64GB; | |
| Pamięć masowa | SSD 256GB M.2 NVMe | |
| Grafika | Zintegrowana z procesorem powinna umożliwiać pracę dwumonitorową, współdzielona i dynamicznie przydzielana pamięć z RAM | |
| Matryca | Rozmiar matrycy | Matowa, IPS, 23,8” |
| Rozdzielczość | FHD (1920x1080) |
| Jasność typowa | 250 cd/m² |
| Kontrast typowy | 700:1 |
| Kąty widzenia pion/poziom | 178( stopni; |
| Rozmiar plamki | Maksymalnie 0,28 mm; |
| Wyposażenie multimedialne | Karta dźwiękowa zintegrowana z płytą główną;  Wbudowane dwa głośniki 2W na kanał.  Wbudowana w obudowę matrycy cyfrowa kamera 2,0 MP z diodą LED informującą użytkownika o pracy. Mechaniczna chowana w obudowie (nie dopuszcza się kamer przekręcanych i wystających poza obrys obudowy)  Wbudowane w obudowę dwa mikrofony | |
| Obudowa | Musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej lub kłódki (oczko w obudowie do założenia kłódki);  Demontaż tylnej pokrywy musi odbywać się bez użycia narzędzi;  Komputer musi posiadać możliwość zainstalowania na ścianie przy wykorzystaniu ściennego systemu montażowego VESA;  Suma wymiarów obudowy z zainstalowanym standem nie może przekraczać: 120cm  Suma wymiarów obudowy bez zainstalowanego standu nie może przekraczać: 100cm  Zasilacz wewnętrzny o mocy 220W o efektywności 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 80% przy obciążeniu zasilacza na poziomie 100%,  Wbudowany w obudowie wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, w szczególności: uszkodzenia lub braku pamięci RAM, uszkodzenia płyty głównej, awarii procesora. System musi zapisywać logi zdarzeń w BIOS. System diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów wymaganych w specyfikacji.  Komputer musi być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz wpisanym na stałe w BIOS.  Podstawa jednostki typu All – in – One musi umożliwiać:  Regulację pochyłu pionowego w zakresie od -5 do 30 stopni.  Regulację wysokości w zakresie minimum 10 cm. | |
| Zgodność z systemami operacyjnymi i standardami | Oferowane modele komputerów muszą współpracować z oferowanymi systemami operacyjnymi – załączyć do oferty wydruk ze strony internetowej producenta oprogramowania; | |
| Zdalne zarządzanie | Wbudowana w płytę główną technologia zarządzania i monitorowania komputera na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6, a także zapewniająca:  - Monitorowanie konfiguracji komponentów komputera - CPU, Pamięć, HDD wersja BIOS płyty głównej;  - Zdalną konfigurację ustawień BIOS,  - Zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego;  - Zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nieulotnej.  - Technologia zarządzania i monitorowania komputerem na poziomie sprzętowym powinna być zgodna z otwartymi standardami DMTF WS-MAN (http://www.dmtf.org/standards/wsman) oraz DASH (http://www.dmtf.org/standards/mgmt/dash/). | |
| Bezpieczeństwo | Płyta główna zawierająca 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  Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub szybkiego menu boot’owania, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów bez konieczności uruchamiania systemu operacyjnego. System musi posiadać wszystkie swoje funkcjonalności w przypadku: braku dysku, uszkodzenia dysku, sformatowania dysku, braku dostępu do sieci, internetu. Nie dopuszcza się stosowania wewnętrznych i zewnętrznych urządzeń w celu uzyskania funkcjonalności systemu diagnostycznego.  Czujnik otwarcia obudowy, musi zbierać zdarzenia i zapisywać je w BIOS | |
| Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu. | |
| BIOS | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo lub nazwę producenta komputera lub nazwę modelu oferowanego komputera.  Pełna obsługa BIOS za pomocą myszy, w tym możliwość swobodnego poruszania się po menu we/wy oraz wł/wy funkcji bez używania klawiatury;  Informacje dostępne z poziomu BIOS na potrzeby inwentaryzacji: wersja BIOS, nr seryjny, data produkcji komputera, pamięć RAM (taktowanie, wielkość, obsadzenie kości w slotach), procesor (typ, nazwa, prędkość) , pojemności zainstalowanych dysków twardych, MAC adres zintegrowanej karty sieciowej, zintegrowany układ graficzny, kontroler audio. Informacje te musza być dostępne w samym menu BIOS bez stosowania dodatkowego oprogramowania jak i wbudowanego systemu diagnostycznego.  Możliwość, ustawienia hasła na poziomie administratora i użytkownika;  Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń.  Możliwość wyłączenia/włączenia karty sieciowej, kontrolera SATA, kontrolera audio, układu TPM, wbudowanej kamery i czytnika kart multimedialnych  Możliwość włączenia/wyłączenia czujnika otwarcia obudowy, ustawienia go w tryb cichy  Możliwość przypisania w BIOS numeru nadawanego przez administratora oraz możliwość weryfikacji tego numeru w oprogramowaniu diagnostyczno-zarządzającym.  Możliwość zdefiniowania automatycznego uruchamiania komputera w wybrane dni tygodnia,  Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne.  Możliwość wyłączania portów USB w szczególności pojedynczo w dowolnej kombinacja.  BIOS musi nanosić automatycznie wszystkie zmiany konfiguracji dotyczące w szczególności: pamięci, procesora, dysku. | |
| Certyfikaty i standardy | Komputer musi być wyprodukowany zgodnie z normami ISO9001 i ISO50001 – **certyfikaty załączyć do oferty;** | |
| Wbudowane porty | 1x DP++ 1.4/HDCP  1x USB 3.2 Typ-C  1 x USB 3.2 Typ A  2 x USB 2.0 Typ A  Nie dopuszcza się stosowania rozgałęziaczy, hub’ów itp.  1x Universal audio jack  1x One Line-out audio  1x RJ-45 port 10/100/1000 Mbps  Czytnik kart SD 4.0  Karta WiFi ac+ bluetooth 5  Płyta główna wyposażona w 2 złącza DIMM z obsługą do 64GB DDR4 pamięci RAM, 1 złącze M.2 dla dysku twardego oraz 1 złącze M.2 karty WiFi  Klawiatura USB w układzie polski programisty  Mysz optyczna USB z dwoma przyciskami oraz rolką (scroll) | |
| 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.  W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego;  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: 2. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, 3. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 4. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego 5. Interfejs użytkownika dostępny w języku polskim i angielskim 6. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 7. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 8. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z poziomów: menu, otwartego okna systemu operacyjnego; 9. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 10. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 11. Graficzne środowisko instalacji i konfiguracji w języku polskim 12. Wbudowany system pomocy w języku polskim. 13. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 14. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora Zamawiającego. 15. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 16. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, w tym możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 17. Zabezpieczony hasłem hierarchiczny dostęp do systemu; 18. Konta i profile użytkowników zarządzane zdalnie; 19. Praca systemu w trybie ochrony kont użytkowników. 20. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze; 21. Molliwość zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 22. 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 23. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 24. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 25. Oprogramowanie dla tworzenia kopii zapasowych (Backup); 26. Automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 27. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 28. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 29. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu); 30. Wbudowany mechanizm wirtualizacji typu hypervisor; 31. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem interfejsu graficznego. 32. Bezpłatne biuletyny bezpieczeństwa związane z działaniem systemu operacyjnego. 33. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; 34. Zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 35. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny; 36. Zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej i udostępnianiem plików; 37. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. 38. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi i niezarządzanymi. 39. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne; 40. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 41. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych; 42. Możliwość tworzenia wirtualnych kart inteligentnych. 43. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 44. Wsparcie dla IPSEC oparte na politykach; 45. Wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; 46. Mechanizmy logowania w oparciu o: 47. Login i hasło, 48. Karty inteligentne i certyfikaty (smartcard), 49. Wirtualne karty inteligentne i certyfikaty chronione poprzez moduł TPM; 50. 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,   1. Kompresja danych, 2. Transmisja po bezpiecznym protokole TLS, 3. Deklaracja klucza szyfrującego dane użytkownika, 4. Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji, 5. Obliczanie sumy kontrolnej, 6. Kopie zapasowe musza być przechowywane w data center, na terenie   Polski.   1. Licencje muszą być przypisywane do urządzenia z limitem pojemności   przestrzeni w chmurze minimum 50 GB;   1. Wsparcie techniczne, świadczone w języku polskim; 2. **M**onitorowanie komputera i generowanie zgłoszeń o błędach / nieprawidłowym działaniu w zakresie pracy komponentów i wydajności systemów 3. Powiadamianie o nowych wersjach sterowników i umożliwienie użytkownikowi wykonania upgrade systemu 4. Powiadamianie o problemach wydajnościowych i diagnozowanie /   rozwiązywanie takich problemów   1. Śledzenie kluczowych komponentów i przewidywanie awarii przed ich   wystąpieniem.   1. Upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w   obrazie systemu operacyjnego, BIOS’u z certyfikatem zgodności  producenta do najnowszej dostępnej wersji;   1. Mozliwość sprawdzenia każdego sterownika, aplikacji, BIOS’u   bezpośrednio na stronie producenta przed instalacją oraz uzyskanie  informacjio:   * 1. poprawkach i usprawnieniach dotyczących aktualizacji   2. dacie wydania ostatniej aktualizacji   3. priorytecie aktualizacji   4. zgodności z systemami operacyjnymi   5. jakiego sprzętu dotyczy aktualizacja  1. Uzyskanie wylazu najnowszych aktualizacji z podziałem na krytyczne, rekomendowane i opcjonalne 2. Włączenie/wyłączenie funkcji automatycznego restartu; 3. Rozpoznanie modelu oferowanego komputera, numeru seryjnego,   uzyskanie informacj kiedy dokonany został ostatnio upgrade;   1. Sprawdzenie historii upgrade’ów z informacją jakie sterowniki były   instalowane;   1. Uzyskanie wykazu wymaganych sterowników, aplikacji, BIOS’u z   informacją o zainstalowanej obecnie wersji;   1. Uzyskanie raportu uwzględniającego informacje o : sprawdzaniu   aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach, zainstalowanych aktualizacjach | |

1. **Laptopy – 7 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” LED IPS FHD o rozdzielczości 1920x1080, z powłoką matową; |
| Wydajność | Oferowany komputer musi osiągać w teście wydajności BAPCO Sysmark 25 wynik 1000 pkt. **Wydruk z oprogramowania testującego załączyć do oferty.**  Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS ( tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.).  Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów Oferent musi dostarczyć Zamawiającemu oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego |
| Pamięć RAM | 8GB DDR4 z możliwością rozbudowy do 20GB; |
| Pamięć masowa | 256GB SSD;  Dysk twardy musi zawierać partycję recovery, a na partycji musi znajdować się obraz zainstalowanych i skonfigurowanych elementów tj.:  - systemu operacyjnego  - oprogramowania użytkowego  Partycja musi zapewniać przywrócenie systemu operacyjnego, zainstalowanego i skonfigurowanego w/w oprogramowania.  Możliwość instalacji wewnątrz obudowy drugiego dysku 2.5. |
| Grafika | Musi umożliwiać pracę dwumonitorową ze wsparciem DirectX 12, OpenGL 4.5; |
| Karta dźwiękowa | Karta dźwiękowa zgodna z HD Audio, wbudowane dwa głośniki stereo oraz dwa cyfrowe mikrofony |
| Wbudowane połączenia i karty sieciowe | Karta sieciowa LAN 10/100/1000 LAN  WLAN 802.11 ax wraz z Bluetooth 5.0 |
| Porty/złącza  (wbudowane) | 1x Czytnik Kart pamięci SD lub microSD  2x USB 3.2, w tym 1 x Type-C  2x USB 2.0  1x Gniazdo mikrofonowe/Gniazdo słuchawkowe (Combo)  1x HDMI ze wsparciem HDCP |
| Klawiatura | Pełnowymiarowa klawiatura z wydzielonymi pełnowymiarowymi klawiszami numerycznymi w prawej części klawiatury, w układzie US-QWERTY, polskie znaki zgodne z układem MS Windows "polski programistyczny", klawiatura podświetlana musi być wyposażona w 2 klawisze ALT (prawy i lewy). |
| Urządzenie wskazujące | Touch Pad (płytka dotykowa) wbudowana w obudowę notebooka. |
| Kamera | Wbudowana, o parametrach:  HD 1280x720, 720p HD audio/video nagrywanie.  Wbudowane dwa kierunkowe mikrofony. |
| Bateria i zasilanie | 35Whr.  Czas pracy na baterii - 6 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 maksymalnie 90W; |
| Waga i wymiary | Maksymalnie 1,8 kg. |
| Obudowa | Wzmocniona, szkielet wykonany ze wzmocnionego aluminium. |
| 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 | - Zabezpieczenie BIOS hasłem użytkownika.  - Zabezpieczenie dysku twardego hasłem użytkownika.  - ZTPM 2.0 |
| Warunki gwarancyjne | Gwarancja producenta komputera - 36 miesięcy  Wymagane okno czasowe dla zgłaszania usterek min. wszystkie dni robocze w godzinach od 8:00 do 20:00. Zgłoszenie serwisowe przyjmowane poprzez stronę www lub telefoniczne (dedykowany numer serwisowy do obsługi zgłoszeń serwisowych. Oferent musi posiadać ISO 9001 i ISO27001 na serwis rozwiązań informatycznych – **certyfikat załączyć do oferty** |
| Wsparcie techniczne producenta | A) Dostęp do aktualizacji systemu BIOS, podręczników użytkownika, najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta komputera numeru seryjnego lub modelu komputera – do oferty należy dołączyć link strony.  B) Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach przy użyciu dedykowanego darmowego oprogramowania producenta lub bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera po podaniu numeru seryjnego komputera lub modelu Komputera. |
| System operacyjny | System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:   1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: 2. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, 3. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 4. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego 5. Interfejs użytkownika dostępny w języku polskim i angielskim 6. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 7. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 8. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z poziomów: menu, otwartego okna systemu operacyjnego; 9. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 10. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 11. Graficzne środowisko instalacji i konfiguracji w języku polskim 12. Wbudowany system pomocy w języku polskim. 13. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 14. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora Zamawiającego. 15. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 16. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, w tym możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 17. Zabezpieczony hasłem hierarchiczny dostęp do systemu; 18. Konta i profile użytkowników zarządzane zdalnie; 19. Praca systemu w trybie ochrony kont użytkowników. 20. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze; 21. Molliwość zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 22. 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 23. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 24. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 25. Oprogramowanie dla tworzenia kopii zapasowych (Backup); 26. Automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 27. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 28. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 29. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu); 30. Wbudowany mechanizm wirtualizacji typu hypervisor; 31. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem interfejsu graficznego. 32. Bezpłatne biuletyny bezpieczeństwa związane z działaniem systemu operacyjnego. 33. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; 34. Zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 35. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny; 36. Zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej i udostępnianiem plików; 37. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. 38. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi i niezarządzanymi. 39. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne; 40. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 41. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych; 42. Możliwość tworzenia wirtualnych kart inteligentnych. 43. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 44. Wsparcie dla IPSEC oparte na politykach; 45. Wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; 46. Mechanizmy logowania w oparciu o: 47. Login i hasło, 48. Karty inteligentne i certyfikaty (smartcard), 49. Wirtualne karty inteligentne i certyfikaty chronione poprzez moduł TPM; 50. 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; |

1. **Serwer Typ I – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| Obudowa | Obudowa Rack o wysokości max 1U z możliwością instalacji 10 dysków 2,5” typu hot-swap. |
| Płyta główna | Możliwość instalacji dysków SAS/SATA/NVMe   * Przystosowana do pracy ciągłej, dedykowana do pracy w serwerach; * Serwer musi posiadać zintegrowany w płycie głównej aktywny układ zgodny ze standardem Trusted Platform Module (min. TPM v 1.2) * Slot PCIe gen 3 przeznaczony dla dysku z interfejsem M.2 * 10 slotów SATA3 |
| Procesor | Osiągający w teście PassMark CPU Mark wynik 11 100 – załączyć do oferty wydruk ze strony <https://www.cpubenchmark.net/> |
| RAM | 64GB pamięci RAM ECC RDIMM;  Płyta musi obsługiwać 1,5TB pamięci RAM;  Na płycie głównej musi znajdować się 6 slotów przeznaczonych dla pamięci. |
| Karta graficzna | Zintegrowana karta graficzna umożliwiająca rozdzielczość. 1920 x 1200 |
| Wbudowane porty | 6 portów USB w tym 1 port wewnątrzny,  2 porty USB 3.0 z tyłu obudowy,  1 port VGA oraz port RS-232 na tylnym panelu.  Nie dopuszcza się stosowania konwerterów/przejściówek. |
| Gniazda PCI | 3 sloty PCIe gen3, z czego 2 sloty umożliwiające instalację karty o pełnym wymiarze wysokości i długości; |
| Interfejsy sieciowe | Wbudowane 2 porty 10Gb Ethernet (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)  Wbudowane 2 porty 1Gb Ethernet;  Wbudowany 1 port Gigabit Ethernet RJ-45 dedykowany dla karty zarządzającej |
| Kontroler dysków | Dedykowany kontroler dyskowy SAS 12Gb/s, wyposażony w minimum 2GB pamięci cache.  Możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. |
| Dyski twarde | Zainstalowane 4 dyski SAS o pojemności 960 GB, 7.2RPM, Hot-Plug klasy Enterprise.  Zainstalowane 4 dysk SSD SATA o pojemności min. 960GB, 6Gbps, Hot-Plug klasy Enterprise,  Możliwość zainstalowania jednego dysku M.2 NVMe |
| Zasilacze | 2 redundantne zasilacze hot-plug, o mocy 750W o sprawności 94% przy 50% obciążeniu, 90% sprawności przy 100% obciążeniu. |
| Wentylatory | 5 wentylatorów |
| Bezpieczeństwo | * Możliwość wyłączenia w BIOS funkcji przycisku zasilania. * BIOS musi mieć możliwość przejścia do bezpiecznego trybu rozruchowego * Możliwość włączania I wyłączania portów USB na obudowie * Wbudowany czujnik otwarcia obudowy * Wbudowany moduł TPM min. v 1.2 * Możliwość zapisywania i odtwarzania ustawień firmware w BIOS |
| Diagnostyka | Umieszczone na froncie obudowy lampki LED, umożliwiający wyświetlenie informacji o stanie: dysków twardych, połączenia sieciowego, zasilaniu, pamięci RAM i temperaturze. |
| Certyfikaty | Serwer musi być wyprodukowany zgodnie z normą ISO-9001, ISO 27001 i ISO 28001 - **załaczyć do oferty certyfikaty**. |
| Warunki gwarancji | 5 lat gwarancji on site producenta serwera, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia;  W przypadku awarii dyski zostają u zamawiającego  Serwis musi być świadczony zgodnie z normą ISO 27001 – **załaczyć do oferty certyfikat dla oferenta;** |

1. **Serwer Typ II – 1 szt**.

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| Obudowa | Obudowa Rack o wysokości max 1U z możliwością instalacji 8 dysków 2,5” typu hot-swap. |
| Płyta główna | Możliwość instalacji dysków SAS/SATA/NVMe   * Przystosowana do pracy ciągłej, dedykowana do pracy w serwerach 2 procesorowych; * Serwer musi posiadać zintegrowany w płycie głównej aktywny układ zgodny ze standardem Trusted Platform Module (min. TPM v 1.2) * 1 slot PCIe gen 3 przeznaczony dla dysku z interfejsem M.2 * 8 slotów SATA3 |
| Procesor | Dwa procesory osiągające współnie w teście PassMark CPU Mark wynik 19 400 – załączyć do oferty wydruk ze strony <https://www.cpubenchmark.net/> |
| RAM | 64GB pamięci RAM ECC RDIMM;  Płyta musi obsługiwać 3 TB pamięci RAM;  Na płycie głównej musi znajdować się 12 slotów przeznaczonych dla pamięci. |
| Karta graficzna | Zintegrowana karta graficzna umożliwiająca rozdzielczość. 1920 x 1200 |
| Wbudowane porty | 4 porty USB 3.0 z tyłu obudowy,  1 port VGA;  Nie dopuszcza się stosowania konwerterów/przejściówek. |
| Gniazda PCI | 1 slot PCIe gen3 umożliwiając instalację karty o pełnym wymiarze wysokości i połowie długości; |
| Napęd optyczny | Możliwość instalacji wewnętrznego napędu DVD-ROM. |
| Interfejsy sieciowe | Wbudowane 2 porty 1Gb Ethernet (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)  Wbudowane. 2 porty 1Gb Ethernet;  Wbudowany 1 port Gigabit Ethernet RJ-45 dedykowany dla karty zarządzającej |
| Kontroler dysków | Dedykowany kontroler dyskowy SAS 12Gb/s, wyposażony w minimum 2GB pamięci cache.  Możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. |
| Dyski twarde | Zainstalowane 4 dyski SAS o pojemności 960 GB, 7.2RPM, Hot-Plug klasy Enterprise.  Zainstalowane 4 dysk SSD SATA o pojemności 960GB, 6Gbps, Hot-Plug klasy Enterprise,  Możliwość zainstalowania jednego dysku M.2 NVMe |
| Zasilacze | 2 redundantne zasilacze hot-plug, o mocy 750W o sprawności 94% przy 50% obciążeniu, 90% sprawności przy 100% obciążeniu. |
| Wentylatory | 4 wentylatory |
| Bezpieczeństwo | * Możliwość wyłączenia w BIOS funkcji przycisku zasilania. * BIOS musi mieć możliwość przejścia do bezpiecznego trybu rozruchowego * Możliwość włączania I wyłączania portów USB na obudowie * Wbudowany czujnik otwarcia obudowy * Wbudowany moduł TPM min. v 1.2 * Możliwość zapisywania i odtwarzania ustawień firmware w BIOS |
| Diagnostyka | Umieszczone na froncie obudowy lampki LED, umożliwiający wyświetlenie informacji o stanie: dysków twardych, połączenia sieciowego, zasilaniu, pamięci RAM i temperaturze. |
| Certyfikaty | Serwer musi być wyprodukowany zgodnie z normą ISO-9001, ISO 27001 i ISO 28001 - **załaczyć do oferty certyfikaty**. |
| Warunki gwarancji | 5 lat gwarancji on site producenta serwera, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia;  W przypadku awarii dyski zostają u zamawiającego  Serwis musi być świadczony zgodnie z normą ISO 27001 – **załaczyć do oferty certyfikat dla oferenta;** |

1. **Skaner – 2 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| Typ skanera | płaski |
| Technologia | CIS |
| Źródło światła | LED |
| Rozdzielczość optyczna | 1200 dpi |
| Głębia barw | Kolor: 48 bitów wej./ 24 bitów wyj. Skala szarości: 16 bitów wej./ 8 bitów wyj. Czarno-biały: 1 bit |
| Szybkość skanowania | 8 sek. kolor/mono A3 |
| Obszar skanowania | A3 |
| Komunikacja | USB; |
| Protokół | kompatybilny ze standardem TWAIN |
| Przyciski fizyczne | Umożliwiające skanowanie, OCR, wysyłanie emailem, tworzenia PDFów; |
| Oprogramowanie | Musi umożliwiać:   1. Dostosowanie koloru obrazu, w tym co najmniej: gamma, kontrast, automatyczne przycinanie i automatyczną korektę przekosu; 2. Wysłanie automatyczne zeskanowanych dokumentów do drukarki, klienta poczty e-mail, folderu sieciowego lub na serwer FTP. 3. Zapis zeskanowanych dokumentów do formatów JPEG, TIFF i PDF; |
| Certyfikaty | Energy star – załączyć do oferty; |
| Gwarancja | 12 miesięcy |
| Wymagania dodatkowe | Zdejmowana wierzchnia pokrywa, |

1. **Urządzenie wielofunkcyjne – Typ I – 2 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| Typ drukarki | Laser, mono |
| Funkcje | Drukowanie, Kopiowanie, Skanowanie, Faksowanie |
| Rozmiar wyświetlacza | Wyświetlacz 2-wierszowy |
| Pamięć | 64MB |
| Procesor | 600MHz |
| Komunikacja | USB, LAN; |
| Rozdzielczość kopiowania | 600 x 600dpi |
| Współczynnik powiększenia/ zmniejszenia | 25%-400% |
| Szybkość kopiowania | 30 kopii na minutę |
| Zużycie energii podczas drukowania | Maksymalnie 450W; |
| Poziom hałasu podczas drukowania | Maksymalnie 50dBA; |
| Obslugiwane formaty papieru | A4, Letter, A5, A6; |
| Bezpieczeństwo sieci przewodowej | SMTP-AUTH, SSL/TLS, SNMP v3 |
| Podajnik papieru | 3000 arkuszy; |
| Odbiornik papieru | 100 arkuszy; |
| Szybkość drukowania  2-stronnego | 15 obrazy na minutę |
| szybkość drukowania  1-stronnego | 30 strony na minutę |
| Rozdzielczość drukowania | 1.200 x 1.200dpi, |
| Emulacje | GDI |
| Czas wykonania pierwszego wydruku | Maksymalnie 10 sekund; |
| Rozdzielczość skanowania | 1.200 x 1,200 dpi; |
| Eksploatacja | Możliwośc zastosowania oryginalnego tonera producenta o wydajności 3 000 stron;  Bęben na 12000 arkuszy; |
| Gwarancja | 3 lata; |
| Wymagania dodatkowe | Automatyczny druk dwustronny, podajnik ręczny, ADF; |

1. **Urządzenie wielofunkcyjne – Typ II – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| Prędkość | 20 stron/min. |
| Dysk wbudowany | 320 GB; |
| Procesor | 1 GHz, dwurdzeniowy; |
| RAM | 4 GB; |
| Komunikacja | 1 GbE, USB 3.0, wifi, wifi direct, NFC; |
| Funkcje kontorlne | książka adresowa, klonowanie konfiguracji, podgląd skanowania, narzędzie zliczania, uprawnienia oparte na rolach, uwierzytelnianie,; |
| Rozdzoieielczość kopiowania/ druku | 600 x 600 dpi /1200 x 2400 dpi; |
| Czas pierwszego wydruku/kopii | Maksymalnie 10 s. mono/kolor |
| Mieisęczne obciążenie zalecane przez producenta | 80 000 stron; |
| Skanowanie | Podgląd skanowania, skanowanie do USB, e-mail, FTP skanowanie formatów plików: PDF, PDF/A, JPG, TIFF, możliwość wyszukiwania PDF, jedno i wielostronicowy PDF/TIFF, PDF chroniony hasłem; |
| Bezpieczeństwo sieciowe | 802.1x, IPsec, HTTPS, SFTP i szyfrowana poczta e-mail, uwierzytelnianie sieciowe, SNMPv3,  SHA-256, TLS 1.1/1.2/1.3, automatyczny certyfikat z podpisem własnym, uwierzytelnianie, FIPS 140-2, zapora wewnętrzna, filtrowanie portów/IP/domeny, kontrola dostępu, TPM; |
| Ochrona danych | Weryfikacja oprogramowania sprzętowego, szyfrowanie na poziomie zadania za pośrednictwem protokołu HTTPS i sterowników, szyfrowana i podpisana poczta e-mail; Zaszyfrowany twardy dysk (256-bitowy AES, FIPS 140-2), |
| Zabezpieczenie dokumentów | Szyfrowane bezpieczne drukowanie, szyfrowanie danych FIPS 140-2; |
| Zarządzanie | Automatyczna konfiguracja ustawień zabezpieczeń, monitorowanie i automatyczne naprawianie, zarządzanie certyfikatami cyfrowymi, interaktywne raporty z pulpitu nawigacyjnego; |
| Języki | PCL5e, PCL6, PDF. XPS, TIFF, JPEG, HP-GL, PostScript; |
| Podajniki papieru - pojemność | 750 arkuszy |
| Odbiorniki papieru - pojemność | 500 arkuszy |
| Gwarancja | 24 miesiące; |
| Wymagania dodatkowe | ADF, duplex, możliwość dostosowania (personalizacji) interfejsu użytkownika, pokazywania i ukrywanie funkcji, uwierzytelnianie, możliwość tworzenia aplikacji jednodotykowych, wbudowany web server, drukowanie z USB, możliwość zapisania pracy, tworzenie broszur, zapisywanie i przywoływanie ustawień sterownika, skalowanie, monitorowanie prac, kontrola aplikacji, drukowanie; |

1. **Zasilacz awaryjny Typ I – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| Rodzaj | Jednofazowy |
| Typ obudowy | Metalowa, rack 2U, konwertowana do Tower, z zestawem montażowym w szafie rack; |
| Topologia | Line-interactive; |
| Rodzaj wejścia | IEC C20; |
| Wyjście | 6 x IEC C13, 2 x IEC C19 zabezpieczone przed przepięciami i bateriami; |
| Kształt fali przy pracy na baterii | Czysty sinus |
| Obciążenie krytyczne i niekrytyczne CL/NCL | 4 |
| Czas transferu | Maksymalnie 5 ms. |
| Przewód zasilający | 2,4 m. |
| Moc wyjściowa VA/W | 3000 |
| Współczynnik mocy | 1 |
| AVR | Double Boost, single buck; |
| Układ przeciwprzepięciowy | Bezpiecznik i ogranicznik |
| Czas pracy na baterii (podtrzymania) | 7 minut przy połowie obciążenia |
| Czas naładowania baterii | Maksymalnie 3h; |
| Zdalne monitorowanie | SNMP/ HTTP |
| Złącza | 1 x EPO, 1 x USB, 1 x port szeregowy, 2 x RJ45; |
| Rozpraszanie ciepła | Maksymalnie 125 BTU/h |
| Hałas | Maksymalnie 60 dBA; |
| Warunki gwarancji | 2 lata na urządzenie, 1 rok na baterie; |
| Wymagania dodatkowe | Certyfikat EnergyStar – **załączyć do oferty,** kompatybilność z aktywnym PFC, technologia EnergySaving, automatyczne wykrywanie częstotliwości wejściowej, obrotowy panel LCD, uruchamianie na baterii, wbudowany moduł zarządzania akumulatorem, możliwość wymiany baterii przez użytkownika, bateria hot-swap, filtrowanie EMI/RFI, styk bezprądowy, kabel USB, szeregowy, EPO, 5 x zasilający; |

1. **Zasilacz awaryjny Typ II – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| Rodzaj | Jednofazowy |
| Typ obudowy | Rack 2U, metalowa, szyny do szafy rack; |
| Topologia | Podwójna konwersja online; |
| Zakres napięcia wejściowego | 200 – 300 Vac, regulowany; |
| Rodzaj wejścia | IEC C20; |
| Wyjście | 8 x IEC C13, 1 x IEC C19, wszystkie zabezpieczone przed przepięciami i bateriami,; |
| Moc | 3000 Vac / 2700 W; |
| Kształt fali | Czysty sinus; |
| Gniazda do obciążeń krytycznych i niekrytycznych CL/NCL | 5/4 |
| Czas transferu | 0 ms. |
| Przewód zasilający | 1,8 m. |
| Współczynnik szczytu | 3:1 |
| Zniekształcenie harmoniczne | THD <5% |
| Układ przecieprzepięciowy | 440J, ochrona sieci LAN (RJ45), |
| Czas pracy na baterii (podtrzymania) | 4 minuty przy pełnym obciążeniu/ 14 minut przy połowicznym; |
| Czas naładowania baterii | Maksymalnie 4h; |
| Zdalne monitorowanie | IPv4/v6, SNMPv1/v3, HTTP/HTTPs, TCP/IP, UDP, DHCP, NTP, DNS, SMTP, SSH, SSL, TLS, Telnet, FTP i Syslog; |
| Złącza | 1 x EPO, 1 x USB, 2 x RJ45; |
| Rozpraszanie ciepła | Maksymalnie 1200 BTU/hr |
| Hałas | Maksymalnie 45 dBA; |
| Warunki gwarancji | 2 lata; |
| Wymagania dodatkowe | Kompatybilność z PFC i generatorem, automatyczne wykrywanie częstotliwości wejściowej i wyjściowej, możliwość konfiguracji napięcia wyjściowego, panel LCD, wewnętrzny ogranicznik prądu, bezpiecznik, ochrona przed przeciążeniem, wewnętrzne obejście ręczne i automatyczne, uruchamianie na baterii, wbudowany moduł zarządzania akumulatorem, możliwość wymiany baterii przez użytkownika, bateria hot-swap, filtrowanie EMI/RFI,obsługa czujnika środowiskowego, kabel USB, 2 x kabel zasilający; |

1. **Oprogramowanie biurowe Typ I – 22 szt.**

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

1. Wymagania odnośnie interfejsu użytkownika:

1. Pełna polska wersja językowa interfejsu użytkownika;
2. Prostota i intuicyjność obsługi, pozwalająca na prace osobom

nieposiadającym umiejętności technicznych;

1. 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:
3. posiada kompletny i publicznie dostępny opis formatu,
4. 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)
5. umożliwia wykorzystanie schematów XML
6. 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)
7. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb użytkownika oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców;
8. W skład oprogramowania muszą wchodzić narzędzia umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami;
9. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim;.
10. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
11. Edytor tekstów
12. Arkusz kalkulacyjny
13. Narzędzie do przygotowywania i prowadzenia prezentacji/ tworzenia, edytowania i wyświetlania prezentacji
14. Narzędzie do zarzadzania informacja prywatną (poczta elektroniczna, kalendarzem, kontaktami i zadaniami)
15. Edytor tekstu musi umożliwiać:
16. 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
17. Wstawianie oraz formatowanie tabel
18. Wstawianie oraz formatowanie obiektów graficznych
19. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne)
20. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków
21. Automatyczne tworzenie spisów treści
22. Formatowanie nagłówków i stopek stron
23. Sprawdzanie pisowni w języku polskim
24. Śledzenie zmian wprowadzonych przez użytkowników
25. Nagrywanie, tworzenie i edycje makr automatyzujących wykonywanie czynności
26. Określenie układu strony (pionowa/pozioma)
27. Wydruk dokumentów
28. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarzadzania informacją prywatną
29. Prace na posiadanych przez zamawiającego dokumentach utworzonych przy pomocy Microsoft Word 2010, 2013 i 2016 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu
30. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
31. 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.
32. 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.
33. 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.
34. Arkusz kalkulacyjny musi umożliwiać:
35. Tworzenie raportów tabelarycznych
36. Tworzenie wykresów liniowych (wraz linia trendu), słupkowych, kołowych
37. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
38. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)
39. Obsługę kostek OLAP oraz tworzenie i edycje kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiazywanie problemów optymalizacyjnych
40. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczna zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych
41. Wyszukiwanie i zamianę danych
42. Wykonywanie analiz danych przy użyciu formatowania warunkowego
43. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
44. Nagrywanie, tworzenie i edycje makr automatyzujących wykonywanie czynności
45. Formatowanie czasu, daty i wartości finansowych z polskim formatem
46. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
47. 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..
48. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
49. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać przygotowywanie prezentacji multimedialnych oraz:
50. Prezentowanie przy użyciu projektora multimedialnego
51. Drukowanie w formacie umożliwiającym robienie notatek
52. Zapisanie w postaci tylko do odczytu.
53. Nagrywanie narracji dołączanej do prezentacji
54. Opatrywanie slajdów notatkami dla prezentera
55. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
56. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
57. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
58. Tworzenie animacji obiektów i całych slajdów
59. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera
60. Pełna zgodność z formatami plików posiadanych przez zamawiającego, utworzonych za pomocą oprogramowania MS PowerPoint 2010, 2013 i 2016.
61. Narzędzie do zarzadzania informacja prywatna (poczta elektroniczna, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
62. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego
63. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców
64. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną
65. Automatyczne grupowanie poczty o tym samym tytule
66. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczna do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy
67. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia
68. Zarzadzanie kalendarzem
69. Udostępnianie kalendarza innym użytkownikom
70. Przeglądanie kalendarza innych użytkowników
71. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach
72. Zarzadzanie lista zadań
73. Zlecanie zadań innym użytkownikom
74. Zarzadzanie listą kontaktów
75. Udostępnianie listy kontaktów innym użytkownikom
76. Przeglądanie listy kontaktów innych użytkowników
77. Możliwość przesyłania kontaktów innym użytkowników
78. Licencja niewygasająca do użytku komercyjnego. Nie dopuszcza się licencji w modelu subskrypcyjnym;
79. **Oprogramowanie bazodanowe – 1 szt.**
80. Środowisko do pracy z dużymi zestawami danych, w tym uczeniem maszynowym i funkcjami sztucznej inteligencji;
81. Odczyt i przetwarzanie dużych zbiorów danych z języka Spark;
82. Łączenie i analiza danych relacyjnych z dużymi zbiorami danych o dużej objętości;
83. Przeszukiwanie zewnętrznych źródeł danych za pośrednictwem klastra;
84. Przechowywanie dużych zbiorów danych w zarządzanym systemie plików HDFS;
85. Wysoka dostępność i odzyskiwanie po awarii baz danych przy użyciu wbudowanej technologii;
86. Wykonywanie zapytań o dane z zewnętrznych źródeł danych za pomocą tabel zewnętrznych z [obsługą kodowania UTF-8](https://docs.microsoft.com/en-us/sql/relational-databases/collations/collation-and-unicode-support?view=sql-server-ver15);
87. Funkcja udzielania opinii w trybie wsadowym;
88. Dostosowanie rozmiarów przydziałów pamięci dla operatorów trybu wsadowego i wierszowego;
89. Możliwość korygowania nadmiernych i niewystarczających przydziałów, które powodują marnowanie pamięci;
90. Wykonywanie w trybie wsadowym bez wymagania indeksów magazynu kolumn;
91. Automatyczne przekształcanie skalarne UDF w wyrażenia relacyjne i osadzanie ich w wywołującym zapytaniu, poprawiające wydajność obciążeń korzystających ze skalarnych funkcji UDF;
92. Odroczona kompilacja zmiennych tabeli;
93. Przybliżone przetwarzanie zapytania w scenariuszach, w których czas reakcji jest krytyczny;
94. Hybrydowa pula buforów;
95. Metadane musąa być zoptymalizowane pod kątem pamięci;
96. Obsługa OLTP w pamięci dla migawek bazy danych;
97. Wymuszanie szybkiego przewijania do przodu i statyczne kursory;
98. Szczegółowa kontrola limitów pamięci;
99. Ograniczanie liczby ponownych kompilacji obciążeń;
100. Skalowalność punktów kontrolnych;
101. Równoczesna aktualizacje PFS;
102. Musi pokazywać skumulowany czas na poziomie instancji poświęcony na synchroniczne operacje odświeżania statystyk;
103. Licencja na serwer oraz 11 licencji dostępowych na urządzenia w sieci;
104. Możliwość dostosowaania gromadzenia danych na określonym serwerze;
105. Funkcja zarządzania, która zwraca odpowiednik ostatniego znanego rzeczywistego planu wykonania dla wszystkich zapytań;
106. Zmiana konfiguracji zakresu bazy danych;
107. Narzędzie zwracające informację o stronie w bazie danych;
108. Środowisko programistyczne z ulepszeniami wykresów i typów danych przestrzennych, obsługą UTF-8 i strukturą rozszerzalności, która pozwala programistom używać wybranego języka w celu uzyskania wglądu w wszystkie swoje dane;
109. Możliwość zdefiniowania kaskadowych operacji usuwania ograniczenia krawędzi;
110. Możliwość znalezienia najkrótszej ścieżki między dwoma dowolnymi węzłami na wykresie lub wykonania przemierzania o dowolnej długości;
111. Tabele wykresów muszą obsługiwać partycjonowanie tabel i indeksów;
112. Możliwość używania tabeli pochodnej lub aliasów widoku w zapytaniu dopasowującym wykres;
113. Obsługa UTF-8 do importowania i eksportowania kodowania oraz jako sortowanie danych ciągów na poziomie bazy danych lub kolumny;
114. Pakiet SDK języka Java;
115. Środowisko wykonawcze Java;
116. Identyfikatory odniesień przestrzennych;
117. Szyfrowanie w miejscu z zaawansowanymi obliczeniami, umożliwiające obliczenia na danych w postaci zwykłego tekstu w bezpiecznej enklawie po stronie serwera;
118. Obsługa zaawansowanych obliczeń takich jak dopasowywanie wzorców i operacje porównywania;
119. Narzedzie do zarządzania certyfikatami;
120. **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. 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);

1. Mozliwość przywrócenia plików, folderów lub całego serwera z kopii zapasowej be zużycia innych plikacji;
2. Backup przyrostowy;
3. Przesyłanie informacji o zmianach plikach do chmury;
4. Optymalizacja wykorzystania przepustowaości sieci LAN i WAN;
5. Backup komputerów klienckich podłączonych do sieci zmożliwościa jego konfiguracj i jego odtwarzaniei;
6. Kreator naprawy kopii zapasowej bazy danych;
7. Reset do ustawień domyślnych i czyszczenie kopii zapasowej;
8. Zarządzanie urządzeniami sieciowymi za pomocą pulpitu nawigacyjnego serwera;
9. Możliwośc stworzenia biblioteki multimediów;
10. Zarządzanie dyskami twardymi za pomocą pulpitu nawigacyjnego
11. Przeprowadzanie kontroli i napraw dysków twardych;
12. Formatowanie dysków twardych
13. Dodawanie nowego dysku twardego;
14. Licencja na 2 CPU i 64 GB RAMu;
15. Możliwość uruchomienia zarównio w postci fizycznej jak wirtualnej;
16. **Tablet – 15 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| Procesor | Ośmiordzeniowy, taktowanie 2.0 GHz; |
| Ekran | 11 cali, IPS, o rozdzielczości 2000 x 1200, 10 punktów dotyku; |
| Jasność ekranu | 400 nitów; |
| Grafika | Zintegrowana zprocesorem, 800 MHz; |
| RAM | 4 GB DDR4; |
| Dysk | 64 GB z możliwością rozbudowy do 1 TB; |
| Aparat wbudowany | Przód – 8 Mpix, tył – 13 Mpix. |
| Mikrofony wbudowane | 2 szt. |
| Komunikacja | 1 x USB 3.o typ C, 1 x pogo pin, 11a/b/g/n/ac + bluetooth 5.1 |
| Głośniki wbudowane | 4 x 1W z technologią dźwięku przestrzennego; |
| Czujniki wbudowane | * Przyspieszenia, światła otoczenia, żyroskopowy, Halla, ToF; |
| Bateria wbudowana | 7700 mAh działąjaca oprzez 15 godzin na jednym ładowaniu według materiałów producenta – załączyć do oferty dokument potwierdzający; |
| Ładowanie baterii | Maksymalnie 3 godziny do pełnego naładowania; |
| System operacyjny | Musi umożliwiać:   * + - 1. Zebranie wszystkich wiadomości w jednym miejscu.       2. Przeglądanie, odpowiadamie i kontrolę konwersacji w wielu aplikacjach do przesyłania wiadomości;       3. Wybór osoby do rozmowy;       4. Pojawienie sie rozmów priorytetowych na ekranie blokady;       5. Przypięcie rozmowy, aby zawsze pojawiała się na innych aplikacjach i ekranach.       6. Dostęp do czatu w dowolnym miejscu i czasie;       7. Nagrywanie ekranu z dźwiękiem z mikrofonu, urządzenia lub obu;       8. Wybór tekstu i obrazów z aplikacji;       9. Kopiowanie, zapis i udostęnianie informacji między wieloma aplikacjami;       10. Musi posiadać etykiety na aplikacjach ułatwiające sterowanie telefonem i poruszanie się po nim;       11. Sterowanie głosem również w trybie offline;       12. Podgląd podłączonych urządzeń i zarządzanie nimi;       13. Przełączanie ze słuchawek na głośniki oraz zmianę urządzenia, na którym odtwarzane są multimedia;.       14. Przyznawanie pozwolenia na dostęp do poufnych danych pobieranym aplikacjom;       15. Przyznawanie uprawnień jednorazowych;       16. Automatyczny reset pozwoleń dla niaktywnych aplikacji;       17. Dostarczanie poprawek bezpieczeństwa i prywatności wysyłanych przez producenta;       18. Analizę potencjalnie szkodliwych aplikacji przed ich pobraniem;       19. Skanowanie aplikacji w poszukiwaniu złośliwego oprogramowania;       20. Porównaie haseł wprowadzonych przez użytkownika z listą znanych przejętych haseł oraz powiadamianie użytkownika o dopasowani       21. Używanie używać interfejsów API dla aplikacji do wyciszania wibracji dzwonków, alarmów lub powiadomień;       22. Obsługę aparatu w emulatorze;       23. Wyciszenie urządzenia i powiadomień podczas ładowania;       24. Połączenie aplikacji służbowychh i osobistych w kalendarzu i przypomnieniach       25. Ustawienie harmonogramu automatycznego włączania i wyłączania profilu do pracy       26. Wyświetlanie kart służbowych podczas udostępniania, otwierania aplikacji;       27. Autouzupełnianie poprzez sugestie, które pomogą wypełnić formularze najczęściej używanymi informacjami.       28. Wysyłanie plików i lokalizacji na mapach do urządzeń w pobliżu.       29. Ograniczenie dostępu do pamięci współdzielonej dla wszystkich aplikacji z systemem operacyjnym;       30. Zaplanowanie kiedy urządzenie ma przechodzić w tryb ciemny, akiedy w jasny;       31. Dostępnianie połączenia internetowego przez tethering za pomocą klucza USB Ethernet; |
| Oprogramiowanie zabezpieczające | 1. Oprogramowanie musi pozwalać na pełne skanowanie; 2. Skanowanie w tle 3. Skanowanie w celu wykrycia zagrożeń typu malware 4. Skanowanie karty pamięci 5. Wyznaczanie wyjątków od skanowania na poziomie plików i folderów. 6. Analizowanie zainstalowanych aplikacji na urządzenia pod kątem luk w bezpieczeństwie oraz raportować o wystąpieniu o takiej aplikacji. 7. Harmonogram skanowania 8. Harmonogram skanowania musi wywoływać skanowanie w chwili wykrycia że urządzenie jest ładowane 9. Oprogramowanie musi analizować ustawienia urządzenia w celu minimalizowania zagrożeń oraz przekierowywać do ustawień które powinny być zamienione. 10. Oprogramowanie musi analizować ustawienia co najmniej następujących funkcji:     1. Konta i synchronizacja     2. Bluetooth     3. Szyfrowanie pamięci urządzenia     4. Hotspot i Tethering     5. Blokada ekranu     6. Nieznane źródła aplikacji     7. Debugowanie USB     8. Wi-Fi 11. Oprogramowanie musi analizować i monitorować uprawnienia aplikacji co najmniej do:     1. Dostęp do kontaktów     2. Dostęp do danych identyfikacyjnych     3. Śledzenie lokalizacji     4. Dostęp do wiadomości     5. Dostęp do sieci 12. Oprogramowanie musi chronić przeglądanie Internetu 13. Oprogramowanie musi chronić przez atakami typu Phishing. 14. Oprogramowanie musi posiadać funkcję optymalizacji urządzenia 15. Oprogramowanie musi analizować uruchomione aplikacje i potrafić zamykać aplikacje nieużywane; 16. Oprogramowanie musi wspomagać zarządzanie energią poprzez zamykanie nieużywanych aplikacji, kontrolę jasności ekranu, kontrolę WiFi, bluetooth. 17. Oprogramowanie musi pozwalać na tworzenie co najmniej następujących raportów: wykorzystanie CPU, żywotność baterii oraz wykorzystanie pamięci. 18. Oprogramowanie powinno mieć białą listę aplikacji które nie powinny być zatrzymywane. 19. Oprogramowanie musi posiadać funkcję monitorowania wykorzystania sieci, informowania o zbliżającym się limicie danych oraz blokowania transmisji w przypadku osiągnięcia limitu transmisji danych. 20. Oprogramowanie musi wykonaywać kopię zapasową w chmurz i ja odzyskać; 21. Urządzenie musi posiadać funkcję bezpiecznego usunięcia danych z urządzenia i wszystkich jego nośników. 22. Oprogramowanie musi mieć ochronę rodzicielską o następujących funkcjach: 23. Blokowanie stron po kategoriach (co najmniej: oprogramowanie, media społecznościowe, tylko dla dorosłych) 24. Blokowanie stron ze wskazanego adresu URL. Funkcja musi działać w co najmniej następujących przeglądarkach internetowych: Chrome, Firefox, Maxthon, Opera i Dolphin. 25. Musi posiadać funkcje wyjątków adresów URL 26. Uwierzytelnianie przez odczyt linii papilarnych; 27. Oprogramowanie musi informować o nowych aktualizacjach i ważnych alarmach bezpieczeństwa; 28. Oprogramowanie powinno wykonywać raporty:     1. Znalezione wirusy     2. Zablokowanie połączenia     3. Aktywności związane z ochroną przed kradzieżą     4. Strony internetowe które zostały zablokowane     5. Informacje o kopi zapasowej     6. Informacje o ostatniej aktualizacji bazy wirusów 29. Zdalne pobieranie lokalizacji urządzenia 30. Zdalne usuniecie danych z urządzenia np.: w przypadku kradzieży. 31. Oprogramowanie musi udostępniać kamerę i mikrofon w celu rejestracji w przypadku kradzieży urządzenia. 32. Oprogramowanie powinno w przypadku dwóch nieudanych prób wprowadzenia hasła blokady ekranu, wykonać automatycznie zdjęcie przy wykorzystaniu aparatu na froncie i tyle urządzenia; 33. Oprogramowanie musi posiadać certyfikaty AVTest oraz AV Comparatives Approved mobile produkt. 34. Jeżeli urządzenie jest zablokowanie żadne wiadomości i informacje nie mogą być wyświetlane na ekranie urządzenia. 35. Dział wsparcia dostępny po chat oraz www. 36. Oprogramowanie musi pozwalać na wybranie do jakich danych prywatnych może mogą mieć dostęp aplikacje; 37. Okno pokazujące: zużycie RAM. 38. Możliwość wyłączenia działających w tle aplikacji, 39. Śledzenie zużycia baterii |
| Gwarancja | 12 miesięcy |
| Wymagania dodatkowe | Czytnik kart microSD, 10 punktów dotyku, wodoodporność IP52, EnergyStar 8.0, |

1. **System operacyjny – 24 szt.**

System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

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

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**na zadanie pn.:„Dostawa sprzętu IT i oprogramowania dla potrzeb Urzędu Gminy Brzeźnica i jednostek podległych w ramach projektu „Cyfrowa Gmina”**

**Część II – Dostawa urządzeń zabezpieczających UTM**

- Urządzenia UTM – IPS – sztuk 2

OBSŁUGA SIECI

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.

ZAPORA KORPORACYJNA (Firewall)

1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
3. Urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
4. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
5. Administrator musi mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia.
6. Rozwiązanie musi umożliwiać między innymi filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
7. Administrator ma możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów).
9. Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos).

INTRUSION PREVENTION SYSTEM (IPS)

1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
2. Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
3. Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
4. Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
5. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej.
6. Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.
7. Administrator urządzenia ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
8. Urządzenie ma mieć możliwość ochrony między innymi przed atakami typu SQL injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.

KSZTAŁTOWANIE PASMA (Traffic Shapping)

1. Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
2. Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.
3. Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring).
4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

OCHRONA ANTYWIRUSOWA

1. Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
2. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
3. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
4. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia.

OCHRONA ANTYSPAM

1. Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
2. Ochrona antyspam ma działać w oparciu o:
   1. białe/czarne listy,
   2. DNS RBL,
   3. heurystyczny skaner.
3. W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL.
4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

WIRTUALNE SIECI PRYWANTE (VPN)

1. Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
2. Odpowiednio kanały VPN można budować w oparciu o:
   1. PPTP VPN,
   2. IPSec VPN,
   3. SSL VPN.
3. SSL VPN musi działać w trybach Tunel i Portal.
4. W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.
5. Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
6. Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
7. Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based.

FILTR DOSTĘPU DO STRON WWW

1. Urządzenie ma posiadać wbudowany filtr URL.
2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
3. Administrator musi mieć możliwość dodawania własnych kategorii URL.
4. Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora.
5. Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST.
6. Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji:
7. blokowanie dostępu do adresu URL,
8. zezwolenie na dostęp do adresu URL,
9. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
10. Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
11. Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych.
12. Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS.
13. Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
14. Urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane.

UWIERZYTELNIANIE

1. Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o:
   1. lokalną bazę użytkowników (wewnętrzny LDAP),
   2. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
   3. usługę katalogową Microsoft Active Directory.
2. Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP.
3. Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły:
   1. SSL,
   2. Radius,
   3. Kerberos.
4. Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory.
5. Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta.
6. Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny.

ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

1. Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
2. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
   1. równoważenie względem adresu źródłowego,
   2. równoważenie względem połączenia.
3. Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
4. Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
5. Urządzenie ma posiadać mechanizm statycznego trasowania pakietów.
6. Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
7. Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.
8. Rozwiązanie powinno zapewniać obsługę routingu dynamicznego w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
9. Rozwiązanie powinno wspierać technologię Link Aggregation.

**POZOSTAŁE USŁUGI I FUNKCJE ROZWIĄZANIA**

1. Urządzenie musi posiadać wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci.
2. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay.
3. Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6.
4. Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS.
5. Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3.
6. Urządzenie musi posiadać usługę DNS Proxy.
7. Urządzenie musi posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP).

**ADMINISTRACJA URZĄDZENIEM**

1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
2. Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https.
3. Komunikacja może odbywać się na porcie innym niż https (443 TCP).
4. Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
5. Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana.
6. Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https.
7. Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS).
8. Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX.
9. Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora.
10. Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora.
11. Urządzenie musi posiadać funkcjonalność anonimizacji logów.

**RAPORTOWANIE**

1. Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
3. System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego.
4. System raportujący musi umożliwiać wygenerowanie co najmniej 25 różnych raportów.
5. System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu.
6. W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny.
7. Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy.

**PARAMETRY SPRZĘTOWE**

1. Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 240 GB.
2. Liczba portów Ethernet 10/100/1000Mbps – min. 12.
3. Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G pochodzącego od dowolnego producenta.
4. Przepustowość Firewall – min. 8 Gbps.
5. Przepustowość Firewall wraz z włączonym systemem IPS – min. 3,3 Gbps.
6. Przepustowość filtrowania Antywirusowego – min. 950 Mbps.
7. Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 1,3 Gbps.
8. Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż. 500.
9. Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 100.
10. Obsługa min. VLAN 256.
11. Liczba równoczesnych sesji - min. 500 000 i nie mniej niż 25 000 nowych sesji/sekundę.
12. Urządzenie musi dawać możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
13. Urządzenie jest nielimitowane na użytkowników.