**Załącznik nr 1 do SWZ. Szczegółowy opis przedmiotu zamówienia**

Dotyczy zamówienia publicznego pn. Dostawa sprzętu komputerowego z oprogramowaniem dla Gminy Łuków w ramach projektu „Cyfrowa Gmina”

# Część 1. Dostawa stacji roboczych, zasilaczy awaryjnych, laptopów i oprogramowania

Ogólne warunki realizacji zamówienia

1. Przedmiot zamówienia obejmuje dostarczenie do siedziby Zamawiającego nw. elementów w ilościach wskazanych w zestawieniu rzeczowo - ilościowym poniżej.
2. Dostarczany sprzęt i oprogramowanie muszą być fabrycznie nowe, nieużywane, nieuszkodzone i nieobciążone prawami osób trzecich.
3. Wykonawca zapewni takie opakowanie sprzętu jakie jest wymagane, żeby nie dopuścić do jego uszkodzenia lub pogorszenia jego jakości w trakcie transportu do miejsca dostawy.
4. Sprzęt będzie oznaczony zgodnie z obowiązującymi przepisami, a w szczególności znakami bezpieczeństwa.
5. Wykonawca wyda Zamawiającemu instrukcje obsługi sprzętu lub – jeśli są one udostępniane przez producenta w formie elektronicznej – przekaże adresy WWW, pod którymi można je pobrać.
6. Dla oprogramowania Wykonawca zobowiązany jest do udzielenia niewyłącznej licencji Zamawiającemu lub przeniesienia na Zamawiającego niewyłącznego uprawnienia licencyjnego zgodnego z zasadami licencjonowania określonymi przez producenta.

Zestawienie rzeczowo - ilościowe

|  |  |
| --- | --- |
| Przedmiot dostawy | Ilość |
| Stacje robocze typ A (komputery stacjonarne z systemem operacyjnym i monitorem) | 25 |
| Stacje robocze typ B (komputery stacjonarne z systemem operacyjnym) | 8 |
| Laptopy z systemem operacyjnym | 8 |
| Zasilacze awaryjne do stacji roboczych | 33 |
| Oprogramowanie do zdalnej pracy na stacjach roboczych | 1 |
| Pakiety oprogramowania biurowego | 50 |
| Oprogramowanie antywirusowe | 50 |

Kody CPV:

* + - * 30213000-5 Komputery osobiste
      * 30213100-6 Komputery przenośne
      * 30231300-0 Monitory ekranowe
      * 31682530-4 Awaryjne urządzenia energetyczne
      * 48000000-8 Pakiety oprogramowania i systemy informatyczne
      * 48422000-2 Zestawy pakietów oprogramowania
      * 48600000-4 Pakiety oprogramowania dla baz danych i operacyjne
      * 48900000-7 Różne pakiety oprogramowania i systemy komputerowe

## Stacje robocze typ A (komputery stacjonarne z systemem operacyjnym i monitorem)

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry\*** |
|  |  | Producent, model: ………………………………………………………………… |
| Typ urządzenia | Komputer stacjonarny odpowiedni dla użytkowania aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej. |  |
| Wydajność | Procesor wielordzeniowy, zaprojektowany do pracy w komputerach stacjonarnych, uzyskujący wynik co najmniej 12 000 punktów w teście PassMark - CPU Mark według wyników opublikowanych na stronie <http://www.cpubenchmark.net/cpu_list.php> w okresie nie wcześniej niż 14 dni przed terminem składania ofert.  Do oferty należy załączyć wydruk z ww. strony, dopuszcza się wydruk w języku angielskim. |  |
| Pamięć RAM | Zainstalowane co najmniej 16 GB, możliwość rozbudowy do co najmniej 64 GB, co najmniej jeden wolny slot na moduły pamięci. |  |
| Pamięć masowa | Co najmniej 512 GB NVMe SSD M.2.  Obudowa musi umożliwiać montaż dodatkowego dysku 2.5” lub 3.5”. |  |
| Karta graficzna | Zintegrowana lub dedykowana karta graficzna. |  |
| Wyposażenie multimedialne | Karta dźwiękowa co najmniej dwukanałowa zintegrowana z płytą główną. Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie typu combo (wspólny port słuchawkowo – mikrofonowy), na tylnym panelu co najmniej port audio line-out. |  |
| Obudowa | Typu small form factor (suma wymiarów obudowy nieprzekraczająca 700 mm).  Obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej. Otwory wentylacyjne usytuowane wyłącznie na przednim oraz tylnym panelu obudowy.  Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń bez konieczności użycia narzędzi. Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych) oraz powinna posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym.  Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki).  Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie i wpisanym na stałe w BIOS. |  |
| Zasilacz | Zasilacz o mocy nieprzekraczającej 200W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności co najmniej 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności co najmniej 80% przy obciążeniu zasilacza na poziomie 100%. |  |
| Bezpieczeństwo | 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. Próba usunięcia dedykowanego układu musi prowadzić do uszkodzenia całej płyty głównej. |  |
| BIOS | BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, pełna obsługa za pomocą klawiatury i myszy lub urządzenia wskazującego zintegrowanego w oferowanym urządzeniu. |  |
| Diagnostyka | System diagnostyczny z interfejsem użytkownika dostępny z poziomu BIOS lub z poziomu menu boot, umożliwiający przetestowanie komponentów komputera. |  |
| Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty główej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu). |  |
| System operacyjny | Zainstalowany system operacyjny w wersji odpowiedniej dla administracji samorządowej spełniający następujące wymagania (poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji):  Bezpłatne aktualizacje w ramach wersji systemu operacyjnego przez Internet z możliwością wyboru instalowanych poprawek (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW;  Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu;  Internetowa aktualizacja zapewniona w języku polskim;  Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;  Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe;  Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug &Play, Wi-Fi);  Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer;  Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta;  Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;  Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników;  Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych;  Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych;  Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika;  Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi;  Wbudowany system pomocy w języku polskim;  Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);  Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji;  Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;  Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;  Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji;  Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;  Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach;  Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń;  Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji za logowanego użytkownika celem rozwiązania problemu z komputerem;  Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami (obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową);  Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację;  Graficzne środowisko instalacji i konfiguracji;  Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe;  Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe;  Oprogramowanie dla tworzenia kopii zapasowych (backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej;  Możliwość przywracania plików systemowych;  System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.);  Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu);  Klucz licencyjny zapisany trwale w BIOS, umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego.  Do oferty należy załączyć potwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym (wydruk ze strony producenta systemu operacyjnego, dopuszcza się wydruk w języku angielskim). |  |
| Wymagania dodatkowe | Wbudowane porty – co najmniej:  2 szt. DisplayPort lub 2 szt. HDMI lub 1 szt. DisplayPort i 1 szt. HDMI  Co najmniej 2 porty USB na przednim panelu obudowy.  Co najmniej 4 x USB 3.x typu A na tylnym panelu obudowy.  Port audio typu combo (słuchawki/mikrofon) na przednim panelu obudowy.  Port audio-out na tylnym panelu obudowy.  Port RJ – 45.  Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich ww. portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp. Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej.  Karta sieciowa 10/100/1000 zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika).  Klawiatura USB w układzie polski programisty.  Mysz USB z rolką (scroll).  Nagrywarka DVD +/-RW o prędkości co najmniej 8x.  Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu. |  |
| Ergonomia | Głośność komputera mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego nie może przekraczać 26 dB. Do oferty należy załączyć dokument potwierdzający spełnienie wymagania sporządzony przez laboratorium akredytowane przez Polskie Centrum Akredytacji lub jako dokument równoważny oświadczenie producenta zestawu komputerowego dotyczące głośności tej jednostki. |  |
| Monitor | Ekran o przekątnej co najmniej 27” z powłoką antyrefleksyjną.  Rozdzielczość natywna full HD (1080p) 1920 x 1080 przy 60 Hz.  Jasność: co najmniej 300 cd/m². Kontrast: co najmniej 1000:1.  Kąty widzenia: co najmniej 178/178.  Wbudowane porty: co najmniej VGA oraz HDMI lub DisplayPort.  Wbudowane głośniki stereo.  Wymagany kabel umożliwiający podłączenie do komputera przez porty HDMI lub DisplayPort. |  |
| Warunki gwarancyjne, wsparcie techniczne | Co najmniej pięcioletnia gwarancja producenta, obejmująca wszystkie komponenty komputera i monitor. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego.  Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów.  Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego).  Opcjonalnie wykonawca może zadeklarować nw. warunki świadczenia serwisu gwarancyjnego komputera:   * usługi serwisu gwarancyjnego w miejscu instalacji urządzenia, * czas reakcji serwisu - do końca następnego dnia roboczego.   Ww. opcjonalne warunki świadczenia serwisu gwarancyjnego będą stanowić kryteria oceny ofert. |  |

## Stacje robocze typ B (komputery stacjonarne z systemem operacyjnym)

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry\*** |
|  |  | Producent, model: ………………………………………………………………… |
| Typ urządzenia | Komputer stacjonarny odpowiedni dla użytkowania aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej. |  |
| Wydajność | Procesor wielordzeniowy, zaprojektowany do pracy w komputerach stacjonarnych, uzyskujący wynik co najmniej 12 000 punktów w teście PassMark - CPU Mark według wyników opublikowanych na stronie <http://www.cpubenchmark.net/cpu_list.php> w okresie nie wcześniej niż 14 dni przed terminem składania ofert.  Do oferty należy załączyć wydruk z ww. strony, dopuszcza się wydruk w języku angielskim. |  |
| Pamięć RAM | Zainstalowane co najmniej 16 GB, możliwość rozbudowy do co najmniej 64 GB, co najmniej jeden wolny slot na moduły pamięci. |  |
| Pamięć masowa | Co najmniej 512 GB NVMe SSD M.2.  Obudowa musi umożliwiać montaż dodatkowego dysku 2.5” lub 3.5”. |  |
| Karta graficzna | Zintegrowana lub dedykowana karta graficzna. |  |
| Wyposażenie multimedialne | Karta dźwiękowa co najmniej dwukanałowa zintegrowana z płytą główną. Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie typu combo (wspólny port słuchawkowo – mikrofonowy), na tylnym panelu co najmniej port audio line-out. |  |
| Obudowa | Typu small form factor (suma wymiarów obudowy nieprzekraczająca 700 mm).  Obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej. Otwory wentylacyjne usytuowane wyłącznie na przednim oraz tylnym panelu obudowy.  Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń bez konieczności użycia narzędzi. Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych) oraz powinna posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym.  Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki).  Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie i wpisanym na stałe w BIOS. |  |
| Zasilacz | Zasilacz o mocy nieprzekraczającej 200W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności co najmniej 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności co najmniej 80% przy obciążeniu zasilacza na poziomie 100%. |  |
| Bezpieczeństwo | 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. Próba usunięcia dedykowanego układu musi prowadzić do uszkodzenia całej płyty głównej. |  |
| BIOS | BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, pełna obsługa za pomocą klawiatury i myszy lub urządzenia wskazującego zintegrowanego w oferowanym urządzeniu. |  |
| Diagnostyka | System diagnostyczny z interfejsem użytkownika dostępny z poziomu BIOS lub z poziomu menu boot, umożliwiający przetestowanie komponentów komputera. |  |
| Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty główej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu). |  |
| System operacyjny | Zainstalowany system operacyjny w wersji odpowiedniej dla administracji samorządowej spełniający następujące wymagania (poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji):  Bezpłatne aktualizacje w ramach wersji systemu operacyjnego przez Internet z możliwością wyboru instalowanych poprawek (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW;  Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu;  Internetowa aktualizacja zapewniona w języku polskim;  Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;  Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe;  Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug &Play, Wi-Fi);  Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer;  Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta;  Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;  Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników;  Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych;  Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych;  Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika;  Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi;  Wbudowany system pomocy w języku polskim;  Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);  Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji;  Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;  Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;  Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji;  Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;  Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach;  Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń;  Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji za logowanego użytkownika celem rozwiązania problemu z komputerem;  Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami (obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową);  Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację;  Graficzne środowisko instalacji i konfiguracji;  Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe;  Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe;  Oprogramowanie dla tworzenia kopii zapasowych (backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej;  Możliwość przywracania plików systemowych;  System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.);  Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu);  Klucz licencyjny zapisany trwale w BIOS, umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego.  Do oferty należy załączyć potwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym (wydruk ze strony producenta systemu operacyjnego, dopuszcza się wydruk w języku angielskim). |  |
| Wymagania dodatkowe | Wbudowane porty – co najmniej:  2 szt. DisplayPort lub 2 szt. HDMI lub 1 szt. DisplayPort i 1 szt. HDMI  Co najmniej 2 porty USB na przednim panelu obudowy.  Co najmniej 4 x USB 3.x typu A na tylnym panelu obudowy.  Port audio typu combo (słuchawki/mikrofon) na przednim panelu obudowy.  Port audio-out na tylnym panelu obudowy.  Port RJ – 45.  Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich ww. portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp. Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej.  Karta sieciowa 10/100/1000 zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika).  Klawiatura USB w układzie polski programisty.  Mysz USB z rolką (scroll).  Nagrywarka DVD +/-RW o prędkości co najmniej 8x.  Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu. |  |
| Ergonomia | Głośność komputera mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego nie może przekraczać 26 dB. Do oferty należy załączyć dokument potwierdzający spełnienie wymagania sporządzony przez laboratorium akredytowane przez Polskie Centrum Akredytacji lub jako dokument równoważny oświadczenie producenta zestawu komputerowego dotyczące głośności tej jednostki. |  |
| Warunki gwarancyjne, wsparcie techniczne | Co najmniej pięcioletnia gwarancja producenta, obejmująca wszystkie komponenty komputera. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego.  Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów.  Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego).  Opcjonalnie wykonawca może zadeklarować nw. warunki świadczenia serwisu gwarancyjnego komputera:   * usługi serwisu gwarancyjnego w miejscu instalacji urządzenia, * czas reakcji serwisu - do końca następnego dnia roboczego.   Ww. opcjonalne warunki świadczenia serwisu gwarancyjnego będą stanowić kryteria oceny ofert. |  |

## Zasilacze awaryjne do stacji roboczych

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry\*** |
|  |  | Producent, model: ………………………………………………………………… |
| Typ urządzenia | Zasilacz awaryjny w obudowie typu tower |  |
| Moc | Co najmniej 210W, moc pozorna co najmniej 325VA |  |
| Topologia | Line-interactive |  |
| Czas podtrzymania | 25 min. dla obciążenia 50% lub więcej  7 min. dla obciążenia 100% lub więcej |  |
| Gniazda | Co najmniej 4 x IEC 320 C13 |  |
| Komunikacja | USB |  |
| Sygnalizacja | Diody LED |  |
| Zabezpieczenia | Przeciwprzepięciowe  Termiczne  Zabezpieczenie przed rozładowaniem |  |
| Gwarancja | Co najmniej 2-letnia gwarancja producenta. |  |

## Laptopy z systemem operacyjnym

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry\*** |
|  |  | Producent, model: ………………………………………………………………… |
| Typ urządzenia | Komputer mobilny odpowiedni dla użytkowania aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej. |  |
| Ekran | Przekątna 15,6”, rozdzielczość co najmniej full HD (1920 x 1080), powłoka przeciwodblaskowa, jasność co najmniej 250 nitów, kontrast co najmniej 700:1. |  |
| Wydajność | Procesor wielordzeniowy, zaprojektowany do pracy w komputerach przenośnych, uzyskujący wynik co najmniej 10 000 punktów w teście PassMark - CPU Mark według wyników procesorów publikowanych na stronie <http://www.cpubenchmark.net/cpu_list.php> w okresie nie wcześniej niż 14 dni przed terminem składania ofert.  Do oferty należy załączyć wydruk z ww. strony, dopuszcza się wydruk w języku angielskim. |  |
| Pamięć RAM | Zainstalowane co najmniej 16 GB, możliwość rozbudowy do co najmniej 32 GB, co najmniej jeden wolny slot na moduły pamięci. |  |
| Pamięć masowa | Co najmniej 256GB NVMe SSD M.2. |  |
| Karta graficzna | Karta graficzna zintegrowana lub dedykowana. |  |
| Karta sieciowa | Zintegrowana, 10/100/1000 (RJ-45) dostępna bezpośrednio z obudowy bez konieczności używania dodatkowych adapterów. |  |
| Multimedia | Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki stereo.  Port audio typu combo (wspólne złącze obsługujące słuchawki i mikrofon).  Wbudowana kamera co najmniej 720p z mechaniczną przysłoną.  Czytnik kart czytający co najmniej karty micro SD. |  |
| Łączność bezprzewodowa | Wi-Fi generacji co najmniej 6  Bluetooth standardu co najmniej 5.1 |  |
| Bateria i zasilanie | Bateria co najmniej 45 Whr, umożliwiająca jej szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin.  Zasilacz dedykowany przez producenta. |  |
| Waga | Nie więcej niż 2 kg z baterią. |  |
| Obudowa | Szkielet obudowy i zawiasy notebooka wzmacniane, dookoła matrycy uszczelnienie chroniące klawiaturę notebooka po zamknięciu przed kurzem i wilgocią. |  |
| BIOS | BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, pełna obsługa za pomocą klawiatury i myszy lub urządzenia wskazującego zintegrowanego w oferowanym urządzeniu. |  |
| Diagnostyka | System diagnostyczny z interfejsem użytkownika dostępny z poziomu BIOS lub z poziomu menu boot, umożliwiający przetestowanie komponentów komputera. |  |
| Bezpieczeństwo | Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu musi powodować uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej.  Czytnik linii papilarnych. |  |
| System operacyjny | Zainstalowany system operacyjny w wersji odpowiedniej dla administracji samorządowej spełniający następujące wymagania (poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji):  Bezpłatne aktualizacje w ramach wersji systemu operacyjnego przez Internet z możliwością wyboru instalowanych poprawek (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW;  Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu;  Internetowa aktualizacja zapewniona w języku polskim;  Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;  Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe;  Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug &Play, Wi-Fi);  Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer;  Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta;  Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;  Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników;  Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych;  Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych;  Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika;  Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi;  Wbudowany system pomocy w języku polskim;  Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);  Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji;  Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;  Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;  Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji;  Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;  Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach;  Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń;  Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji za logowanego użytkownika celem rozwiązania problemu z komputerem;  Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami (obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową);  Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację;  Graficzne środowisko instalacji i konfiguracji;  Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe;  Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe;  Oprogramowanie dla tworzenia kopii zapasowych (backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej;  Możliwość przywracania plików systemowych;  System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.);  Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu);  Klucz licencyjny zapisany trwale w BIOS, umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego.  Do oferty należy załączyć potwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym (wydruk ze strony producenta systemu operacyjnego, dopuszcza się wydruk w języku angielskim). |  |
| Klawiatura | Klawiatura z wydzieloną częścią numeryczną, podświetlana.  Touchpad z dwoma przyciskami. |  |
| Porty i złącza | Wbudowane porty i złącza – co najmniej:  1 szt. HDMI,  1 szt. RJ-45,  3 szt. USB (w tym co najmniej 1 szt. USB 3.x i 1 szt. USB 3.x z zasilaniem),  1 szt. USB 3.x typu C z zasilaniem,  port zasilania (nie zajmujący portu USB typ C),  złącze linki zabezpieczającej. |  |
| Warunki gwarancyjne, wsparcie techniczne | Co najmniej pięcioletnia gwarancja producenta obejmująca wszystkie komponenty komputera. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego.  Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów.  Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego).  Opcjonalnie wykonawca może zadeklarować nw. warunki świadczenia serwisu gwarancyjnego:   * usługi serwisu gwarancyjnego w miejscu instalacji urządzenia, * czas reakcji serwisu - do końca następnego dnia roboczego.   Ww. opcjonalne warunki świadczenia serwisu gwarancyjnego będą stanowić kryteria oceny ofert. |  |

*\* W kolumnie „Oferowane parametry” należy podać rzeczywiste parametry oferowanego sprzętu, tj. np.:*

* *„Zainstalowane 12 GB”, a nie „Zainstalowane co najmniej 12 GB”;*
* *„Dysk SSD o pojemności 512 GB”, a nie „Dysk SSD o pojemności co najmniej 256 GB”.*

*W przypadku oprogramowania dostarczanego z oferowanymi urządzeniami należy podać producenta i nazwę oprogramowania, nie ma konieczności uzupełniania listy cech i funkcji oprogramowania.*

## Pakiety oprogramowania biurowego

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane oprogramowanie** |
|  |  | Producent, nazwa oprogramowania: ………………………………………………………………… |
| Zawartość pakietu | Pakiet musi zawierać:   * edytor tekstów, * arkusz kalkulacyjny, * narzędzie do przygotowania i prowadzenia prezentacji, * narzędzie do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami). |  |
| Wymagania ogólne dla pakietu | Wymagana pełna polska wersja językowa interfejsu użytkownika, w tym także systemu interaktywnej pomocy w języku polskim. Pakiet powinien mieć system aktualizacji darmowych poprawek bezpieczeństwa, przy czym komunikacja z użytkownikiem powinna odbywać się w języku polskim.  Dostępność w Internecie na stronach producenta biuletynów technicznych, w tym opisów poprawek bezpieczeństwa, w języku polskim, a także telefonicznej pomocy technicznej producenta pakietu biurowego świadczonej w języku polskim w dni robocze w godzinach od 8 do 17 – cena połączenia nie większa niż cena połączenia lokalnego.  Wymagany publicznie znany cykl życia przedstawiony przez producenta dotyczący rozwoju i wsparcia technicznego – w szczególności w zakresie bezpieczeństwa co najmniej 5 lat od daty zakupu.  Możliwość dostosowania pakietu aplikacji biurowych do pracy dla osób niepełnosprawnych np. słabo widzących, zgodnie z wymogami Krajowych Ram Interoperacyjności (WCAG 2.0).  Wymagane dostarczenie licencji odpowiedniej dla jednostek samorządu terytorialnego.  Licencja musi obejmować najnowszą wersję systemu dostępną na dzień składania oferty. |  |
| Edytor teksu | Edytor tekstu musi umożliwiać:   * Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty. * Wstawianie oraz formatowanie tabel. * Wstawianie oraz formatowanie obiektów graficznych. * Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne). * Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków. * Automatyczne tworzenie spisów treści. * Formatowanie nagłówków i stopek stron. * Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie. * Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. * Określenie układu strony (pionowa/pozioma). * Wydruk dokumentów. * Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną. * Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. * 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. |  |
| Arkusz kalkulacyjny | Arkusz kalkulacyjny musi umożliwiać:   * Tworzenie raportów tabelarycznych. * Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych. * Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu. * Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice). * Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. * Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych. * Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych. * Wyszukiwanie i zamianę danych. * Wykonywanie analiz danych przy użyciu formatowania warunkowego. * Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie. * Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. * Formatowanie czasu, daty i wartości finansowych z polskim formatem. * Zapis wielu arkuszy kalkulacyjnych w jednym pliku. * Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. |  |
| Narzędzie do przygotowywania i prowadzenia prezentacji | Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:   * Przygotowywanie prezentacji multimedialnych, które mogą być prezentowanie przy użyciu projektora multimedialnego. * Drukowanie w formacie umożliwiającym robienie notatek. * Zapisanie jako prezentacja tylko do odczytu. * Nagrywanie narracji i dołączanie jej do prezentacji. * Opatrywanie slajdów notatkami dla prezentera. * Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo. * Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego. * Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym. * Możliwość tworzenia animacji obiektów i całych slajdów. * Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera. |  |
| Narzędzie do zarządzania informacją prywatną | Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:   * Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego. * Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych. * Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców. * Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną. * Automatyczne grupowanie poczty o tym samym tytule. * Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy. * Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów. * Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie. * Zarządzanie kalendarzem. * Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników. * Przeglądanie kalendarza innych użytkowników. * Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach. * Zarządzanie listą zadań. * Zlecanie zadań innym użytkownikom. * Zarządzanie listą kontaktów. * Udostępnianie listy kontaktów innym użytkownikom. * Przeglądanie listy kontaktów innych użytkowników. * Możliwość przesyłania kontaktów innym użytkowników. |  |

## Oprogramowanie do zdalnej pracy na stacjach roboczych

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane oprogramowanie** |
|  |  | Producent, nazwa oprogramowania: ………………………………………………………………… |
| Licencja | Wymagane dostarczenie licencji na oprogramowanie do bezpiecznego zdalnego dostępu na stacjach roboczych (dalej: Oprogramowanie) zlokalizowanych w jednostce Zamawiającego. Jedna licencja musi pozwalać na dostęp do co najmniej 30 urządzeń zarządzanych. W przypadku dostarczenia licencji ograniczonej czasowo licencja powinna umożliwiać korzystanie z oprogramowania przez co najmniej 3 lata. |  |
| Funkcjonalność | * Oprogramowanie musi umożliwiać przejęcie zdalnej kontroli nad innym urządzeniem, na którym jest zainstalowane to oprogramowanie. * Musi istnieć możliwość zainstalowania Oprogramowania jako usługi systemowej. * Oprogramowanie musi pozwalać na bezpośrednie połączenia LAN przez TCP/IP i kanał wirtualnej sieci prywatnej (VPN). * Oprogramowanie musi działać przez zapory ogniowe i automatycznie wykrywać dowolną konfigurację serwera proxy. * Oprogramowanie musi wykrywać urządzenia znajdujące się w pobliżu. * Oprogramowanie musi posiadać funkcje umożliwiające komunikację z użytkownikami sieci, np. w formie czatu. * Oprogramowanie musi umożliwiać nawiązanie wielu połączeń jednocześnie i przełączanie się między nimi. * Oprogramowanie musi obsługiwać zdalne budzenie komputera (Wake-on-LAN), oraz zdalny restart z automatycznym wznowieniem połączenia. * Oprogramowanie musi umożliwiać wygaszanie ekranu komputera zdalnego. * Oprogramowanie musi umożliwić obsługę kilku ekranów komputera zdalnego. * Oprogramowanie musi dla zapewnienia bezpieczeństwa połączeń:   + wykorzystywać algorytm wymiany kluczy publicznych/prywatnych RSA 2048 i szyfrowania sesji w systemie E2EE zgodnie ze standardem AES (256-bitowy),   + wykorzystywać losowe hasła jednorazowego dostępu,   + umożliwiać uwierzytelnianie dwuskładnikowe,   + umożliwiać zdefiniowanie zaufanych urządzeń i kontrolę dostępu poprzez zaufane urządzenia,   + umożliwiać stosowanie białych list. * Oprogramowanie musi umożliwiać zapisywanie ustawień połączeń. * Oprogramowanie musi umożliwiać zdalne uaktualnienia i instalację. |  |
| Kompatybilność | * Oprogramowanie musi zapewniać połączenia pomiędzy różnymi platformami: z komputera PC na komputer PC, z urządzenia mobilnego na komputer PC, z komputera PC na urządzenie mobilne, z urządzenia mobilnego na urządzenie mobilne. * Oprogramowanie musi zapewniać połączenia z urządzeniami pracującymi pod kontrolą systemów: Windows 10/8.1/7, Windows Server 2019/2012/2008R2, macOS 10.11 i nowsze, Linux, Chrome OS, iOS, Android. |  |

## Oprogramowanie antywirusowe

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane oprogramowanie** |
|  |  | Producent, nazwa oprogramowania: ………………………………………………………………… |
| Licencja | Pakiet oprogramowania antywirusowego w wersji polskiej z subskrypcją 3-letnią posiadający pełne wsparcie dla systemu operacyjnego Microsoft Windows 10 i nowszych. |  |
| Funkcjonalność | 1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 3. Wbudowana technologia do ochrony przed rootkitami. 4. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 7. System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania. 8. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 9. Możliwość skanowania dysków sieciowych i dysków przenośnych. 10. Skanowanie plików spakowanych i skompresowanych. 11. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 12. Wykluczenie ze skanowania musi odbywać się nie tylko po nazwie pliku ale również ma być możliwe użycie symbolu wieloznacznego „\*” zastępującego dowolne znaki w ścieżce. 13. Administrator ma możliwość dodania wykluczenia po tzw. HASH’u zagrożenia, wskazującego bezpośrednio na określoną infekcję a nie konkretny plik. 14. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. 15. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu. 16. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera. 17. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji. 18. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. 19. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej. 20. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy ww. klientów poczty. 21. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 22. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. 23. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. 24. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. 25. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony. 26. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora. 27. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 28. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 29. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego. 30. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. 31. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło. 32. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo. 33. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów. 34. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku. 35. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym. 36. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, optycznych pamięci masowych, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 37. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia, dana funkcjonalność musi pozwalać na automatyczne wypełnienie właściwości urządzenia dla tworzonej reguły. 38. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie brak dostępu do podłączanego urządzenia. 39. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 40. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. 41. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). 42. Moduł HIPS musi działać co najmniej w trybie automatycznym, tzn. program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika. 43. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego. 44. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania akcji blokuj lub zezwól. 45. Oprogramowanie musi posiadać zaawansowany skaner pamięci. 46. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp. 47. Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie. 48. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu. 49. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur. 50. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji. 51. Program musi być wyposażony w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback). 52. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 53. Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania. 54. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. 55. Program musi posiadać możliwość aktywacji poprzez podanie klucza licencyjnego oraz możliwość aktywacji programu offline. 56. Możliwość podejrzenia licencji za pomocą której program został aktywowany. 57. W programie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji. 58. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej. 59. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika. 60. Aplikacja musi posiadać funkcję ręcznej aktualizacji komponentów programu. |  |

# Część 2. Dostawa urządzenia wielofunkcyjnego

Ogólne warunki realizacji zamówienia

1. Przedmiot zamówienia obejmuje dostarczenie do siedziby Zamawiającego nw. elementów w ilościach wskazanych w zestawieniu rzeczowo - ilościowym poniżej.
2. Dostarczany sprzęt i oprogramowanie muszą być fabrycznie nowe, nieużywane, nieuszkodzone i nieobciążone prawami osób trzecich.
3. Wykonawca zapewni takie opakowanie sprzętu jakie jest wymagane, żeby nie dopuścić do jego uszkodzenia lub pogorszenia jego jakości w trakcie transportu do miejsca dostawy.
4. Sprzęt będzie oznaczony zgodnie z obowiązującymi przepisami, a w szczególności znakami bezpieczeństwa.
5. Wykonawca zainstaluje urządzenie będące przedmiotem dostawy oraz uruchomi je i przeprowadzi instruktaż z obsługi urządzenia dla pracowników wskazanych przez Zamawiającego.
6. Wykonawca wyda Zamawiającemu instrukcje obsługi sprzętu lub – jeśli są one udostępniane przez producenta w formie elektronicznej – przekaże adresy WWW, pod którymi można je pobrać.
7. Dla oprogramowania Wykonawca zobowiązany jest do udzielenia niewyłącznej licencji Zamawiającemu lub przeniesienia na Zamawiającego niewyłącznego uprawnienia licencyjnego zgodnego z zasadami licencjonowania określonymi przez producenta.

Zestawienie rzeczowo - ilościowe

|  |  |
| --- | --- |
| Przedmiot dostawy | Ilość |
| Urządzenie wielofunkcyjne | 1 |

Kody CPV:

* + - * 42962000-7 Urządzenia drukujące i graficzne
      * 30121430-6 Cyfrowe urządzenia powielające

## Urządzenie wielofunkcyjne

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry\*** |
|  |  | Producent, model: ………………………………………………………………… |
| Typ urządzenia | Urządzenie wielofunkcyjne - drukowanie, kopiowanie, skanowanie |  |
| Technologia druku | Laserowa monochromatyczna |  |
| Maksymalny obsługiwany format (dotyczy druku i skanowania) | A3 lub większy |  |
| Rozdzielczość druku | Do 1200 x 1200 dpi lub większa |  |
| Maksymalna szybkość drukowania | Do 25 stron A4/min. lub więcej |  |
| Optyczna rozdzielczość skanowania | Do 600x600 dpi lub większa |  |
| Szybkość skanowania automatycznego | 70 obrazów na minutę (300 dpi, A4) lub więcej  35 obrazów na minutę (300 dpi, A4) lub więcej dla skanowania dwustronnego |  |
| Funkcje | Skanowanie w kolorze i w odcieniach szarości  Skanowanie do e-mail, skanowanie do PDF, skanowanie do USB host, Local/Network TWAIN, WIA |  |
| Rozdzielczość kopiowania | 600 x 600 dpi lub większa |  |
| Zakres skalowania | W zakresie co najmniej od 25% do 400% |  |
| Maksymalna gramatura nośników | Do 220 g/m² lub więcej |  |
| Pojemność podajnika automatycznego oryginałów (ADF) | Do 100 arkuszy lub więcej  Dopuszczalna gramatura do 220 g/m² lub więcej |  |
| Pojemność podajników papieru | Zainstalowane co najmniej 2 kasety na papier po 500 arkuszy lub więcej (dla A4, 80 g/m²).  Taca wielofunkcyjna na co najmniej 100 arkuszy (dla A4, 80 g/m²). |  |
| Pojemność odbiornika papieru | Do 3 000 arkuszy lub więcej (dla A4, 80 g/m²). |  |
| Obsługiwane formaty nośników | Co najmniej A3, A4, A4R, A5R, B4, B5, B5R |  |
| Pamięć masowa | Co najmniej 250 GB |  |
| Komunikacja | Co najmniej: USB i 2 x USB Host, Gigabit Ethernet (10BaseT/100BaseTX/ 1000BaseT) |  |
| Sterowanie | Wyświetlacz dotykowy o przekątnej co najmniej 10 cali |  |
| Obsługiwane systemy operacyjne | Wszystkie aktualnie wspierane wersje Microsoft Windows |  |
| W zestawie wymagane | Oryginalny toner pozwalający na wydruk co najmniej 40 000 stron |  |
| Gwarancja | Co najmniej 2-letnia gwarancja producenta.  Wykonawca może zaoferować dłuższy okres gwarancji. Okres gwarancji stanowi jedno z kryteriów oceny ofert. |  |

*\* W kolumnie „Oferowane parametry” należy podać rzeczywiste parametry oferowanego sprzętu, tj. np.:*

* *„Zainstalowane 12 GB”, a nie „Zainstalowane co najmniej 12 GB”;*
* *„Dysk SSD o pojemności 512 GB”, a nie „Dysk SSD o pojemności co najmniej 256 GB”.*

# Część 3. Dostawa sprzętu serwerowego i sieciowego z oprogramowaniem

Ogólne warunki realizacji zamówienia

1. Przedmiot zamówienia obejmuje dostarczenie do siedziby Zamawiającego nw. elementów w ilościach wskazanych w zestawieniu rzeczowo - ilościowym poniżej.
2. Dostarczany sprzęt i oprogramowanie muszą być fabrycznie nowe, nieużywane, nieuszkodzone i nieobciążone prawami osób trzecich.
3. Wykonawca zapewni takie opakowanie sprzętu jakie jest wymagane, żeby nie dopuścić do jego uszkodzenia lub pogorszenia jego jakości w trakcie transportu do miejsca dostawy.
4. Sprzęt będzie oznaczony zgodnie z obowiązującymi przepisami, a w szczególności znakami bezpieczeństwa.
5. Wykonawca zainstaluje w szafie rack urządzenia będące przedmiotem dostawy oraz uruchomi je i skonfiguruje w porozumieniu z Zamawiającym.
6. Wykonawca wyda Zamawiającemu instrukcje obsługi sprzętu lub – jeśli są one udostępniane przez producenta w formie elektronicznej – przekaże adresy WWW, pod którymi można je pobrać.
7. Dla oprogramowania Wykonawca zobowiązany jest do udzielenia niewyłącznej licencji Zamawiającemu lub przeniesienia na Zamawiającego niewyłącznego uprawnienia licencyjnego zgodnego z zasadami licencjonowania określonymi przez producenta.

Zestawienie rzeczowo - ilościowe

|  |  |
| --- | --- |
| Przedmiot dostawy | Ilość |
| Oprogramowanie do tworzenia kopii zapasowych (backup) | 1 |
| Urządzenie dyskowe NAS (backup) | 1 |
| Serwer z systemem operacyjnym | 1 |
| Szafa rack | 1 |
| Serwerowy zasilacz awaryjny | 1 |
| Urządzenie UTM | 1 |

Kody CPV:

* + - * 48820000-2 Serwery
      * 30233000-1 Urządzenia do przechowywania i odczytu danych
      * 31213300-5 Szafy kablowe
      * 32420000-3 Urządzenia sieciowe
      * 48000000-8 Pakiety oprogramowania i systemy informatyczne
      * 48422000-2 Zestawy pakietów oprogramowania
      * 48600000-4 Pakiety oprogramowania dla baz danych i operacyjne
      * 48900000-7 Różne pakiety oprogramowania i systemy komputerowe

## Oprogramowanie do tworzenia kopii zapasowych (backup)

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane oprogramowanie** |
|  |  | Producent, nazwa oprogramowania: ………………………………………………………………… |
| Licencja, wymagania ogólne | Wymagane dostarczenie licencji odpowiedniej dla serwera będącego przedmiotem zamówienia. Jeśli licencja jest przypisana do serwerów wirtualnych, należy uwzględnić konieczność obsługi co najmniej dwóch serwerów wirtualnych.  Licencja musi ponadto umożliwiać tworzenie kopii zapasowych na 50 stacjach roboczych.  Oprogramowanie w języku polskim i możliwość uzyskania pomocy technicznej w języku polskim. |  |
| Funkcjonalność - tworzenie kopii zapasowych | 1. Możliwość backupu obejmującego kopie całego systemu operacyjnego wraz z konfiguracją oraz zainstalowanymi aplikacjami i plikami. 2. Możliwość skonfigurowania różnych schematów wykonywania backupu: w trybie pełnym, backupy przyrostowe lub tryb mieszany. Harmonogram przyrostowy powinien umozliwiać backup z częstotliwością min. co 15 minut. 3. Możliwość wykonywania backupów pełnych i przyrostowych na dyski lokalne, dyski sieciowe, SAN, NAS, dyski USB, Firewire. 4. Możliwość wykonywania kopie zapasowe (backupy) na poziomie sektorów, czyli backup przyrostowy, zawierający tylko zmienione sektory na dysku, a nie np. całe pliki. 5. Program nie może wymagać oddzielnego serwera zarządzającego backupem, a harmonogram zadań tworzenia backupów dla danej maszyny ma być przechowywany bezpośrednio na tej maszynie. 6. Tworzenie kopii zapasowej w automatycznym trybie hot backupu (bez korzystania ze skryptów zamykających i uruchamiających bazy czy programy). Hot backup powinien pozwalać na backup systemu, aplikacji i baz danych takich jak MS SQL, MS Exchange, Active Directory, Share Point, Oracle od wersji 11g. 7. Możliwość wykonywania kopii zapasowej dysku bez konieczności uruchamiania systemu operacyjnego za pomocą bootowalnej płyty lub pendrive’a z systemem i oprogramowaniem dostarczanym przez producenta rozwiązania backupowego. 8. Rozwiązanie musi pozwalać na okresową weryfikację, konsolidację oraz retencję łańcucha backupu przyrostowego z możliwością konfiguracji po jakim czasie mają się one wykonać. 9. Rozwiązanie musi umożliwiać tworzenie backupu przez łącze 3G i WiFi. 10. Podczas tworzenia kopii zapasowej program musi generować plik sumy kontrolnej (md5) dla pliku backupu w celu kontroli plików backupu. 11. Program musi posiadać narzędzie pozwalające na automatyczną weryfikację tworzonych plików backupu za pomocą okresowego uruchamiania backupowanego systemu operacyjnego w maszynie wirtualnej, oraz wysłanie zrzutu ekranu z tak uruchomionego systemu do administratora za pomocą wiadomości email. 12. Program musi umożliwiać konwersje kopii zapasowej do plików dysków maszyn wirtualnych w formacie VHD, VMDK, VHDX. 13. Program musi umożliwiać replikację wykonanych plików kopii zapasowych na dyski lokalnie, dyski sieciowe lub do lokalizacji zdalnych na serwer FTP. |  |
| Funkcjonalność - przywracanie z kopii zapasowych | 1. Możliwość przywrócenia backupu całego obrazu dysku/partycji na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników do nowego sprzętu lub możliwość dodania sterowników przez użytkownika. Komputer powinien zostać uruchomiony z bootowalnej płyty CD lub pendrive’a, z którego bezpośrednio zostaje uruchomiony proces odzyskiwania obrazu dysku z backupu. 2. Program musi pozwalać na dowolne odtwarzanie maszyn fizycznych na inną fizyczną lub do maszyny wirtualnej oraz z maszyny wirtualnej do innej maszyny wirtualnej lub na fizyczną. 3. Bez względu na rozmiar backupu, program musi umożliwiać automatyczne uruchomienie systemu z backupu jako maszyny wirtualnej w środowiskach VirtualBox, VMware vSphere lub Hyper-V bez konieczności wcześniejszej konwersji pliku backupu do postaci wirtualnej. 4. Program musi umożliwiać zamontowanie pliku backupu jako dysku wirtualnego w trybie odczyt/zapis lub tylko do odczytu. Tak podłączony dysk logiczny umożliwia przeglądanie, wyszukiwanie i odzyskiwanie plików, folderów a także modyfikowanie zawartości. 5. Podczas przywracania obrazu dysku/partycji z kopii zapasowej, program musi umożliwiać: uaktywnienie wybranej partycji, przywrócenia sektora MBR, przywrócenie sygnatur dysku, przywrócenie ukrytych ścieżek na dysku, dezaktywację licencji systemu Windows. 6. Program musi pozwalać na zdefiniowanie procesu tworzenia kolejnych backupów przyrostowych, które w sposób automatyczny będą odtwarzane po określonym przez administratora czasie na innej maszynie fizycznej lub wirtualnej (VMDK, VHD, VHDX). Musi istnieć możliwość zdefiniowania opóźnienia z jakim kopie przyrostowe będą przenoszone na nowy wolumin w zakresie od 1 godziny do 30 dni. |  |
| Funkcjonalność – zdalne zarządzanie | 1. Program musi umożliwiać pełną konfigurację i pełne zarządzanie zadaniami wykonywania kopii zapasowej na innych komputerach w sieci lokalnej, w zakresie identycznym jak z lokalnej konsoli administracyjnej. 2. Musi być dostępne narzędzie dające możliwość tworzenia zadań backupu za pomocą polityk dla grup stacji z poziomu konsoli webowej. 3. Konsola webowa musi umożliwiać instalację oraz aktualizację zdalną oprogramowania na punktach końcowych. 4. Konsola webowa musi umożliwiać podgląd dzienników zdarzeń na stacjach końcowych. 5. Program musi umożliwiać wysłanie powiadomień w postaci wiadomości e-mail gdy: zadanie backupu zakończyło się niepowodzeniem, po zakończeniu zadania tworzenia backupu, oraz podsumowanie aktywności dziennej, tygodniowej i miesięcznej. 6. Musi istnieć możliwość pobrania ze strony producenta konsoli zarządzającej w postaci pliku ISO. |  |
| Kompatybilność | Pełne wsparcie dla system operacyjnego zainstalowanego na oferowanym serwerze.  Pełne wsparcie dla środowisk wirtualnych: VMware Workstation, VMware ESX/ESXi, Microsoft Hyper-V, Microsoft Virtual PC, Microsoft Virtual Server.  Wsparcie dla 32 i 64-bitowych systemów Microsoft.  Wsparcie systemów plików: FAT16, FAT16X, FAT32, FAT32X, NTFS.  Wsparcie dla dysków z tablicą partycji MBR oraz GPT  .  Wsparcie systemów plików: ext2, ext3, ext4, XFS.  Wsparcie dla 32 i 64-bitowych systemów Microsoft: Windows 10, Windows 11. |  |

## Urządzenie dyskowe NAS (backup)

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry\*** |
|  |  | Producent, model: ………………………………………………………………… |
| Obudowa | Typu rack, maksymalnie 2 U. |  |
| Pamięć RAM | Zainstalowane co najmniej 4 GB pamięci RAM. Urządzenie musi obsługiwać do 32 GB pamięci RAM lub więcej. |  |
| Obsługa dysków | Wnęka na co najmniej 8 dysków 2,5-calowych lub 3,5-calowych. Wymagana obsługa co najmniej następujących rodzajów dysków: 3,5-calowe dyski twarde SATA, 2,5-calowe dyski twarde SATA, 2,5-calowe dyski SSD SATA. |  |
| Zamontowane dyski | Zamontowane co najmniej 4 dyski o pojemności co najmniej 8 TB każdy, o prędkości obrotowej co najmniej 7200 rpm, prędkości interfejsu co najmniej 6Gbps i deklarowanym średnim czasem bezawaryjnej pracy co najmniej 1 mln godzin. |  |
| RAID | Obsługa RAID co najmniej: 0, 1, 5, 6, 10, JBOD |  |
| Porty | Co najmniej: 4 szt. Ethernet 1GbE (RJ45), 2 szt. USB 3.x., 1 szt. eSATA. |  |
| Zasilanie | Zasilacz wbudowany. |  |
| Wentylacja | Redundantne wentylatory. |  |
| Gwarancja | Co najmniej 2-letnia gwarancja producenta. Dopuszcza się objęcie dysków twardych gwarancją wykonawcy. |  |

## Serwer z systemem operacyjnym

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry\*** |
|  |  | Producent, model: ………………………………………………………………… |
| Obudowa | Typu rack o wysokości maksymalnie 2U z możliwością instalacji do 8 dysków 2.5" Hot-Plug,z kompletem szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli . |  |
| Procesor | Zainstalowany procesor szesnastordzeniowy klasy x86 dedykowany do pracy z zaoferowanym serwerem uzyskujący wynik co najmniej 30 000 punktów w teście PassMark - CPU Mark według wyników opublikowanych na stronie <http://www.cpubenchmark.net/cpu_list.php> w okresie nie wcześniej niż 14 dni przed terminem składania ofert.  Do oferty należy załączyć wydruk z ww. strony, dopuszcza się wydruk w języku angielskim. |  |
| Pamięć RAM | Zainstalowane co najmniej 32 GB pamięci RAM. Płyta główna musi obsługiwać do 1TB pamięci RAM lub więcej. |  |
| Grafika | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości co najmniej 1920x1200. |  |
| Sieć | Wbudowane co najmniej dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT. |  |
| Dyski twarde | Możliwość instalacji dysków SATA, SAS, SSD.  Zainstalowane 8 dysków z interfejsem SAS 12Gb/s o pojemności co najmniej 900 GB każdy. |  |
| Kontroler dyskowy | Sprzętowy kontroler dyskowy posiadający co najmniej 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wymagane wsparcie dla dysków samoszyfrujących. |  |
| Porty | Co najmniej 4 porty USB, 1 port VGA. |  |
| Wentylacja | Redundantne wentylatory. |  |
| Zasilanie | Dwa redundantne zasilacze Hot Plug o mocy maksymalnej nie przekraczającej 800 Wat. |  |
| Diagnostyka | Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. |  |
| Zarządzanie | Dedykowany moduł zdalnego zarządzania, diagnostyki i monitorowania pracy serwera, niezależny od systemu operacyjnego, posiadający dedykowany port RJ-45 GbE umożliwiający co najmniej:   * + zarządzanie poprzez graficzny interfejs,   + szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika,   + możliwość podmontowania zdalnych wirtualnych napędów,   + wirtualną konsolę z dostępem do myszy, klawiatury,   + integrację z Active Directory,   + wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej,   + możliwość podłączenia lokalnego i bezpośredniego zarządzania poprzez złącze RS-232 lub USB lub microUSB umieszczone na froncie obudowy,   + automatyczne zgłaszanie alertów do centrum serwisowego producenta,   + automatyczne update firmware dla wszystkich komponentów serwera,   + możliwość przywrócenia poprzednich wersji firmware,   + automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram. |  |
| Bezpieczeństwo | * Blokada zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * Możliwość wyłączenia w BIOS funkcji przycisku zasilania. * Możliwość ustawienia w BIOS bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła. * Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. * Moduł TPM 2.0. * Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera. * Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem. |  |
| System operacyjny | System operacyjny spełniający nw. wymagania minimalne:   1. Możliwość wykorzystania procesorów logicznych oraz wirtualnych. 2. Możliwość budowania klastrów, z możliwością uruchamiania maszyn wirtualnych. 3. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 4. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 6. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 7. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 8. Wbudowane wsparcie instalacji i pracy na wolumenach, które:    1. pozwalają na zmianę rozmiaru w czasie pracy systemu,    2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,    3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,    4. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 9. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 10. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 11. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 12. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 13. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 14. Graficzny interfejs użytkownika. 15. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 16. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 17. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 18. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 19. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management). 20. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:     1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,     2. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:        1. Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,        2. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,        3. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.     3. Zdalna dystrybucja oprogramowania na stacje robocze.     4. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej     5. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:        1. Dystrybucję certyfikatów poprzez http        2. Konsolidację CA dla wielu lasów domeny,        3. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.     6. Szyfrowanie plików i folderów.     7. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).     8. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.     9. Serwis udostępniania stron WWW.     10. Wsparcie dla protokołu IP w wersji 6 (IPv6),     11. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,     12. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:     13. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,     14. Obsługi ramek typu jumbo frames dla maszyn wirtualnych,     15. Obsługi 64K sektorów dysków,     16. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,     17. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model). 21. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 22. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). 23. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 24. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji.   Licencja na system operacyjny:   1. musi obejmować najnowszą wersję systemu dostępną na dzień składania oferty, 2. musi uprawniać do uruchamiania co najmniej dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji, 3. musi być zgodna z ilością fizycznych rdzeni procesorowych w serwerze, 4. musi obejmować licencje dostępowe dla 50 użytkowników.   Do oferty należy załączyć potwierdzenie kompatybilności serwera z oferowanym systemem operacyjnym (wydruk ze strony producenta systemu operacyjnego, dopuszcza się wydruk w języku angielskim). |  |
| Warunki gwarancyjne, wsparcie techniczne | Co najmniej pięcioletnia gwarancja producenta, obejmująca wszystkie komponenty serwera. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego.  Możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta. Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów.  Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja serwera, konfiguracja fabryczna, konfiguracja bieżąca, rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego).  Opcjonalnie wykonawca może zadeklarować nw. warunki świadczenia serwisu gwarancyjnego:   * usługi serwisu gwarancyjnego w miejscu instalacji urządzenia, * czas reakcji serwisu - do końca następnego dnia roboczego.   Ww. opcjonalne warunki świadczenia serwisu gwarancyjnego będą stanowić kryteria oceny ofert. |  |
| Dokumentacja | Zamawiający wymaga dokumentacji w języku polskim lub angielskim. |  |
| Wsparcie techniczne | Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |  |

## Szafa rack

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry\*** |
|  |  | Producent, model: ………………………………………………………………… |
| Konstrukcja | Konstrukcja z blachy stalowej, demontowalne ściany boczne |  |
| Wymiary | 42U, 600 x 1000. Szafa musi zostać zamontowana w pomieszczeniu o wysokości 230 cm. |  |
| Nośność | Co najmniej 1200 kg |  |
| Budowa | Perforowane drzwi przednie i tylne.  Drzwi przednie dwudzielne.  Zdejmowane ściany boczne.  Drzwi przednie, tylne i ściany boczne zamykane na zamki.  Otwory na przewody z góry i dołu szafy.  Cztery szyny rack do montażu urządzeń (dwie z przodu, dwie z tyłu), regulacja odległości między szynami. |  |
| Wentylacja | Panel wentylacyjny 4-wentylatorowy. |  |
| Wyposażenie | Należy przewidzieć wyposażenie umożliwiające instalację w szafie i uruchomienie sprzętu będącego przedmiotem zamówienia, tj. serwer, urządzenie NAS, serwerowy zasilacz awaryjny i urządzenie UTM, w tym akcesoria montażowe, przewody i panele / listwy zasilające, patchcordy itp.  Dodatkowo półki – 4 szt.  Złącze uziemiające. |  |

## Serwerowy zasilacz awaryjny

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry\*** |
|  |  | Producent, model: ………………………………………………………………… |
| Typ urządzenia | Zasilacz awaryjny w obudowie typu rack, maksymalnie 4U |  |
| Moc | Co najmniej 1900W, moc pozorna co najmniej 2200VA |  |
| Topologia | Line-interactive |  |
| Czas przełączania | Maksymalnie 4 ms |  |
| Czas podtrzymania | 25 min. dla obciążenia 50% lub więcej  9 min. dla obciążenia 100% lub więcej |  |
| Gniazda | Co najmniej 2 x IEC-C19 i co najmniej 8 x IEC-C13 |  |
| Funkcje i cechy | Automatyczna regulacja napięcia (AVR)  Funkcja korekcji niskich i wysokich napięć  Filtrowanie napięcia  Ładowanie akumulatorów dostosowane do temperatury  Automatyczne włączenie UPS-a po powrocie zasilania  Automatyczny test  Zarządzalne sieciowo  Akumulatory wymienialne przez użytkownika  Akumulatory wymienialne "na gorąco"  Bezpiecznik automatyczny  Regulowane punkty przełączania napięcia  Regulowana czułość na napięcie |  |
| Komunikacja | Port szeregowy  Złącze USB |  |
| Sygnalizacja | Alarmy dźwiękowe  Wskaźnik statusu LED  Powiadomienie o awarii akumulatora  Powiadomienie o rozłączeniu akumulatora |  |
| Gwarancja | Co najmniej 24-miesięczna gwarancja producenta.  Wykonawca może zaoferować dłuższy okres gwarancji. Okres gwarancji stanowi jedno z kryteriów oceny ofert. |  |

## Urządzenie UTM

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry\*** |
|  |  | Producent, model: ………………………………………………………………… |
| Wymagania ogólne | Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza.  System realizujący funkcję firewall musi dawać możliwość pracy w jednym z trzech trybów: routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.  System musi wspierać IPv4 oraz IPv6 w zakresie:  • Firewall.  • Ochrony w warstwie aplikacji.  • Protokołów routingu dynamicznego. |  |
| Redundancja, monitoring i wykrywanie awarii | * + - 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster active-active lub active-passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.  1. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 2. Monitoring stanu realizowanych połączeń VPN. |  |
| Interfejsy | * + - 1. System realizujący funkcję firewall musi dysponować minimum 10 portami Gigabit Ethernet RJ-45.       2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.       3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. |  |
| Wydajność | W zakresie frewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.  Przepustowość stateful firewall: nie mniej niż 10 Gbps dla pakietów 512 B.   1. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. 2. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps. 3. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps. 4. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps. 5. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps. |  |
| Funkcje systemu bezpieczeństwa | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:  Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.  Kontrola Aplikacji.  Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.  Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.  Ochrona przed atakami - Intrusion Prevention System.  Kontrola stron WWW.  Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.  Zarządzanie pasmem (QoS, Traffic shaping).  Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).  Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.  Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.  Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system |  |
| Polityki firewall | Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.  System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:   * + Translację jeden do jeden oraz jeden do wielu.   + Dedykowany ALG (Application Level Gateway) dla protokołu SIP.   W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.  Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP, nazwy domenowe, hashe złośliwych plików.  Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.  • Amazon Web Services (AWS).  • Microsoft Azure  • Google Cloud Platform (GCP).  • OpenStack.  • VMware NSX. |  |
| Połączenia VPN | 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:  * Wsparcie dla IKE v1 oraz v2. * Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). * Obsługa protokołu Diffie-Hellman grup 19 i 20. * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. * Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. * Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. * Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. * Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. * Mechanizm „Split tunneling” dla połączeń Client-to-Site.  1. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:  * Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. * Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. * Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. |  |
| Routing i obsługa łączy WAN | W zakresie routingu rozwiązanie powinno zapewniać obsługę:  • Routingu statycznego.  • Policy Based Routingu.  • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. |  |
| Funkcje SD-WAN | * + - 1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.       2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu. |  |
| Zarządzanie pasmem | 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. |  |
| Ochrona przed malware | 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. |  |
| Ochrona przed atakami | 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 5. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 6. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. |  |
| Kontrola aplikacji | 1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 3. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 4. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. |  |
| Kontrola WWW | 1. Moduł kontroli WWW musi korzystać z bazy adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. |  |
| Uwierzytelnianie użytkowników w ramach sesji | 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:  * Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. * Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. * Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.  1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. 3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |  |
| Zarządzanie | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. |  |
| Logowanie | 1. W ramach logowania system pełniący funkcję firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 2. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 3. Musi istnieć możliwość logowania do serwera SYSLOG. |  |
| Licencje | Z urządzeniem należy dostarczyć licencje upoważniające do korzystania w okresie gwarancji na urządzenie z aktualnych baz funkcji ochronnych producenta i serwisów w zakresie:  kontrola aplikacji, IPS, antywirus (z uwzględnieniem sygnatur do ochrony urządzęń mobilnych - co najmniej dla systemu operacyjnego Android), analiza typu Sandbox, antyspam, web filtering, bazy reputacyjne adresów IP/domen. |  |
| Gwarancja | Co najmniej pięcioletnia gwarancja producenta. |  |