**OPIS PRZEDMIOTU ZAMÓWIENIA - SPRZĘT**

Załącznik do umowy nr…..

Spis treści

[1. Serwer 2](#_Toc116282859)

[2. Serwerowy System Operacyjny 4](#_Toc116282860)

[3. Licencje dostępowe serwera 7](#_Toc116282861)

[4. Przełącznik zasobowy do Macierzy 8](#_Toc116282862)

[5. Macierz 8](#_Toc116282863)

[6. Serwer NAS 10](#_Toc116282864)

[7. Switch 11](#_Toc116282865)

[8. UPS 13](#_Toc116282866)

[9. UPS Stacje robocze 13](#_Toc116282867)

[10. Zestaw komputerowy 14](#_Toc116282868)

[11. Pakiet biurowy 19](#_Toc116282869)

[12. Oprogramowanie wirtualizacyjne 22](#_Toc116282870)

[13. Laptop 22](#_Toc116282871)

[14. Oprogramowanie biurowe 25](#_Toc116282872)

[15. Antywirus 26](#_Toc116282873)

# Serwer

|  |  |  |  |
| --- | --- | --- | --- |
| **Serwer** | | **Ilość** | **1 szt.** |
| **Wymagane minimalne parametry techniczne** | | | |
| **Obudowa** | Obudowa Rack o wysokości max 2U z możliwością instalacji do 8 dysków 2.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.  Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. | | |
| **Płyta główna** | Płyta główna z możliwością zainstalowania minimum dwóch procesorów Intel 3rd Gen. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. | | |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych | | |
| **Procesor** | Zainstalowane dwa procesory 12-rdzeniowe, min. 2.1 GHz (Turbo Speed min. 3.3 GHz), klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie min. 167 punktów w teście SPECrate®2017\_int\_base dla konfiguracji dwuprocesorowej. | | |
| **RAM** | 128GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM. | | |
| **Zabezpieczenia pamięci RAM** | Memory Rank Sparing, Memory Mirror, Failed DIMM isolation | | |
| **Gniazda PCI** | minimum 3 sloty PCIe x16 generacji 4 oraz jeden slot PCIe x4 | | |
| **Interfejsy sieciowe/FC/SAS** | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) wraz z wkładkami SFP+ lub kablami DAC umożliwiające podłączenie dostarczanego serwer do dostarczanych przełączników. | | |
| **Dyski twarde** | Możliwość instalacji dysków SAS, SATA, SSD  Zainstalowane 2 dyski SAS o pojemności min. 900GB 15K RPM Hot-Plug.  Zainstalowane 2 dyski o pojemności min. 480GB SSD Hot-Plug.  Zainstalowany dedykowany modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 32GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. | | |
| **Kontroler RAID** | Sprzętowy kontroler dyskowy posiadający min. 8GB nieulotnej pamięci cache, umożliwiający konfigurację poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków SED. | | |
| **Wbudowane porty** | Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej,  Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0, | | |
| **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 | | |
| **Zasilacze** | Redundantne, Hot-Plug min. 800W każdy | | |
| **Bezpieczeństwo** | * Blokada na ramce panelu zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * Możliwość wyłączenia w BIOS funkcji przycisku zasilania. * BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła * Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. * Moduł TPM 2.0 * Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera * Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem | | |
| **Diagnostyka** | Serwer wyposażony w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. | | |
| **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej; * zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); * szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; * możliwość podmontowania zdalnych wirtualnych napędów; * wirtualną konsolę z dostępem do myszy, klawiatury; * wsparcie dla IPv6; * wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; * możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; * integracja z Active Directory; * możliwość obsługi przez dwóch administratorów jednocześnie; * wsparcie dla dynamic DNS; * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. * możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera | | |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001.  Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019 oraz Microsoft Windows Server 2022. | | |
| **Warunki gwarancji** | Minimalny wymagany okres gwarancji jakości i rękojmi za wady **36 miesięcy** gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.  Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.  Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera | | |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. | | |

# Serwerowy System Operacyjny

|  |  |  |  |
| --- | --- | --- | --- |
| **Serwerowy system operacyjny** | | **Ilość** | **1 kpl.** |
| **Wymagania minimalne** | | | |
| Zamawiający wymaga dostarczenia oprogramowania Windows Server Standard Core 2022, licencja zgodna z oferowaną ilością rdzeni CPU w serwerze lub równoważne. | | | |
| **Opis równoważności** | | | |
| * Licencja ma mieć charakter wieczysty i nie narażać Zamawiającego na dodatkowe koszty w przyszłym użytkowaniu. * Licencja obejmująca wszystkie rdzenie procesorów w zaoferowanym serwerze. * Zamawiający wymaga, aby wszystkie elementy systemu oraz jego licencja pochodziły od tego samego producenta. Licencja ma umożliwiać downgrade do poprzednich wersji systemu operacyjnego oraz uprawniać do uruchamiania SSO w środowisku fizycznym i dwóch wirtualnych środowisk systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. | | | |
| Serwerowy system operacyjny (dalej: SSO) posiada następujące, wbudowane cechy: | | | |
| 1 | Posiada możliwość wykorzystania min. 320 logicznych procesorów oraz min. 4 TB pamięci RAM w środowisku fizycznym | | |
| 2 | Posiada możliwość wykorzystywania min. 64 procesorów wirtualnych oraz min. 1TB pamięci RAM i dysku o pojemności 64TB przez każdy wirtualny serwerowy system operacyjny. | | |
| 3 | Posiada możliwość budowania klastrów składających się z min. 64 węzłów, z możliwością uruchamiania do 7000 maszyn wirtualnych. | | |
| 4 | Posiada możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. | | |
| 5 | Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. | | |
| 6 | Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. | | |
| 7 | Posiada automatyczną weryfikację cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. | | |
| 8 | Posiada możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. | | |
| 9 | Wbudowane wsparcie instalacji i pracy na wolumenach, które:   * pozwalają na zmianę rozmiaru w czasie pracy systemu, * umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, * umożliwiają kompresję „w locie” dla wybranych plików i/lub folderów, * umożliwiają zdefiniowanie list kontroli dostępu (ACL). | | |
| 10 | Posiada wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. | | |
| 11 | Posiada wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. | | |
| 12 | Posiada możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET | | |
| 13 | Posiada możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. | | |
| 14 | Posiada wbudowaną zaporę internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. | | |
| 15 | Graficzny interfejs użytkownika. | | |
| 16 | Zlokalizowane w języku polskim, następujące elementy:   * menu, * przeglądarka internetowa, * pomoc, * komunikaty systemowe. | | |
| 17 | Posiada wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). | | |
| 18 | Posiada możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. | | |
| 19 | Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. | | |
| 20 | Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management). | | |
| 21 | Posiada możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:   * Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, * Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:   + Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,   + Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,   + Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. * Zdalna dystrybucja oprogramowania na stacje robocze. * Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej * Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: * Dystrybucję certyfikatów poprzez http * Konsolidację CA dla wielu lasów domeny, * Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen. * Szyfrowanie plików i folderów. * Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). * Posiada możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów. * Serwis udostępniania stron WWW. * Wsparcie dla protokołu IP w wersji 6 (Ipv6), * Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, * Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtulne 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 zapewniają wsparcie dla: * Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, * Obsługi ramek typu jumbo frames dla maszyn wirtualnych, * Obsługi 4-KB sektorów dysków, * Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, * Posiada możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model) * Posiada 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 | Posiada możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. | | |
| 24 | Posiada mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. | | |
| 25 | Posiada możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. | | |

# Licencje dostępowe serwera

|  |  |  |  |
| --- | --- | --- | --- |
| **Licencje dostępowe serwera** | | **Ilość** | **1 kpl.** |
| **Wymagania minimalne** | | | |
| Windows 2022 50 Device CAL lub równoważne. | | | |
| **Opis równoważności** | | | |
| Sposób licencjonowania | * Licencja ma mieć charakter wieczysty i nie narażać Zamawiającego na dodatkowe koszty w przyszłym użytkowaniu. * Zamawiający wymaga, aby wszystkie elementy systemu oraz jego licencja pochodziły od tego samego producenta. * Licencja ma umożliwiać downgrade do poprzednich wersji licencji oraz uprawniać do dostępu do zasobów serwera dla określonej liczby urządzeń. | | |
| Cechy | Licencja powinna zapewnić (w zgodzie z wymaganiami licencyjnymi producenta) możliwość równoległego zarządzania wybranymi usługami przez administratorów serwera, a także dostęp do zasobów serwera dla 50 urządzeń. | | |
| Kompatybilność | Zamawiający wymaga, aby licencja była kompatybilna z systemem operacyjnym opisanym powyżej. | | |

# Przełącznik zasobowy do Macierzy

|  |  |  |  |
| --- | --- | --- | --- |
| **Przełącznik zasobowy do Macierzy** | | **Ilość** | **2 szt.** |
| **Wymagane minimalne parametry techniczne** | | | |
| **Wysokość** | Max 1U | | |
| **Procesor** | Min. taktowanie 800 MHz | | |
| **Pamięć RAM** | Min. 1GB | | |
| **Pamięć flash** | Min. 16MB | | |
| **Porty** | 1x 10/100/1000 Ethernet  16x SFP+  1x Serial port | | |
| **Zasilanie** | Dwa redundantne zasilacze  Maksymalny pobór urządzenia 45W | | |
| **Normy** | CE, EAC, ROHS | | |
| **Gwarancja** | Min. 12 miesięcy | | |

# Macierz

|  |  |  |  |
| --- | --- | --- | --- |
| **Przełącznik zasobowy do Macierzy** | | **Ilość** | **1 szt.** |
| **Wymagane minimalne parametry techniczne** | | | |
| **Procesor** | Procesor czterordzeniowy 64biotowy o taktowaniu nie niższym niż 2.2GHz | | |
| **Obudowa** | RACK 19" 2U – wraz z kompletem szyn przesuwanych umożliwiającym zamontowanie w szafie RACK | | |
| **Procesor liczba rdzeni** | Nie mniej niż 4 | | |
| **Pamięć RAM** | Minimum 4GB DDR4 ECC | | |
| **Możliwość rozbudowy pamięci RAM do:** | Min. 32 GB | | |
| **Całkowita liczba gniazd pamięci** | 2 | | |
| **Liczba zatok na dyski twarde** | 12 | | |
| **Obsługiwane dyski twarde** | 3.5" oraz 2.5" SATA HDD/SSD – Hot Plug  Zamawiający wymaga dostarczenia 10 dysków 3.5” o pojemności 8TB każdy o parametrach nie gorszych niż:  Prędkość obrotowa: 7200  MTTF: 2 000 000  Obciążenie roczne: 550 TB  Drgania: 0.75 G (od 5 do 300Hz)  Wstrząs: 70 G (czas trwania 2 ms)  Waga: minimum 720 g  Gwarancja producenta dysku: 5 lat  Możliwość aktualizacji oprogramowania dysku z poziomu systemu operacyjnego serwera. | | |
| **Możliwość podłączenia modułu rozszerzającego** | Tak | | |
| **Maksymalna ilość dysków z opcjonalnymi modułami rozszerzającymi, nie mniej niż:** | 24 | | |
| **Porty na karty rozszerzeń** | 1 x Gen3 x8 PCIe (x4 link) | | |
| **Porty LAN** | 4 x RJ-45 1GbE, 2 x 10Gb SFP+ (możliwe zastosowanie dodatkowej karty sieciowej SFP+) | | |
| **Porty USB 3.2** | min. 2 | | |
| **Gniazdo rozszerzenia** | min. 1 | | |
| **Zasilanie** | Redundantny zasilacz o mocy max. 350W | | |
| **Mechanizm szyfrowania sprzętowego** | Tak, min AES-NI | | |
| **Wewnętrzny system plików** | BTRFS, EXT4 | | |
| **Obsługiwane tryby RAID** | JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 | | |
| **Funkcje backup** | Możliwość tworzenia kopii bezpieczeństwa urządzeń pod Windows (Bare Metal), Linux oraz usług chmur publicznych, portal użytkownika do przywracania danych kopii zapasowej (bez uprawnień administratora), backup na zewnętrzne dyski twarde, obsługa minimum 1024 migawek na folder udostępniony, obsługa minimum 65000 migawek na cały system | | |
| **Darmowe aplikacje na urządzenia mobilne** | Monitoring / Zarządzanie / Współdzielenie plików | | |
| **Minimum obsługiwane aplikacje/usługi** | Serwer plików, Serwer FTP, WebDav, Serwer WEB, Serwer kopii zapasowych, Serwer Monitoringu (min. 2 licencje bezpłatne), możliwość utworzenia klastra wysokiej dostępności z 2 identycznych urządzeń, Serwer pocztowy (min. 5 licencji w cenie) | | |
| **VPN** | VPN Server dla min. 40 połączeń | | |
| **Gwarancja producenta na serwer** | Min. 3 lata | | |

# Serwer NAS

|  |  |  |  |
| --- | --- | --- | --- |
| **Serwer NAS** | | **Ilość** | **8 szt.** |
| **Wymagane minimalne parametry techniczne** | | | |
| **Procesor** | Procesor czterordzeniowy 64biotowy o taktowaniu nie niższym niż 2.0GHz | | |
| **Obudowa** | Desktop | | |
| **Procesor liczba rdzeni** | Nie mniej niż 4 | | |
| **Pamięć RAM** | 2GB DDR4 z możliwością rozszerzenia do 6GB | | |
| **Liczba zatok na dyski twarde** | 2  Zamawiający wymaga dostarczenia 2 dysków 3.5” o pojemności 2TB każdy. | | |
| **Całkowita liczba gniazd pamięci** | 1 | | |
| **Kieszenie dysków M.2** | 2 x NVMe | | |
| **Możliwość podłączenia modułu rozszerzającego** | Tak | | |
| **Maksymalna ilość dysków z opcjonalnymi modułami rozszerzającymi, nie mniej niż:** | 7 | | |
| **Porty LAN** | Wbudowane min. 2 x RJ-45 1GbE | | |
| **Porty USB 3.2** | min. 2 | | |
| **Port e-SATA** | min. 1 | | |
| **Zasilanie** | Max. 65W | | |
| **Mechanizm szyfrowania sprzętowego** | Tak, min AES-NI | | |
| **Wewnętrzny system plików** | BTRFS, EXT4 | | |
| **Obsługiwane tryby RAID** | Basic, JBOD, RAID 0, RAID 1 | | |
| **Funkcje backup** | Możliwość tworzenia kopii bezpieczeństwa urządzeń pod Windows (Bare Metal), Linux oraz usług chmur publicznych, portal użytkownika do przywracania danych kopii zapasowej (bez uprawnień administratora), backup na zewnętrzne dyski twarde, obsługa minimum 1024 migawek na folder udostępniony, obsługa minimum 65000 migawek na cały system | | |
| **Darmowe aplikacje na urządzenia mobilne** | Monitoring / Zarządzanie / Współdzielenie plików | | |
| **Minimum obsługiwane aplikacje/usługi** | Serwer plików, Serwer FTP, WebDav, Serwer WEB, Serwer kopii zapasowych, Serwer Monitoringu (min. 2 licencje bezpłatne), możliwość utworzenia klastra wysokiej dostępności z 2 identycznych urządzeń, Serwer pocztowy (min. 5 licencji w cenie) | | |
| **VPN** | VPN Server dla min. 40 połączeń | | |
| **Gwarancja producenta** | Min. 3 lata | | |

# Switch

|  |  |  |  |
| --- | --- | --- | --- |
| **Switch** | | **Ilość** | **4 szt.** |
| **Wymagane minimalne parametry techniczne** | | | |
| **Obudowa** | Do montażu w szafie Rack 19"  Wysokości nie więcej niż 1U, głębokość nie większa niż 30 cm | | |
| **Porty** | Minimum 48 porty GigabitEthernet w standardzie BaseT, minimum 4 zintegrowane porty 10Gb Ethernet SFP+  1x USB Typu A  1x Port konsoli | | |
| **Obsługa adresów MAC** | Min. 16 000 | | |
| **Prędkość przekazywania** | Min. 131 Mpps | | |
| **Zdolność przełączania** | Min. 176 Gbps | | |
| **VLAN** | Obsługa 4094 wirtualnych sieci  Obsługa Protocol based, GVRP, Voice VLAN, Guest VLAN, Private VLAN | | |
| **Funkcjonalności** | IEEE 802.3ad Obsługa do 12 grup agregacji oraz do 8 portów na grupę  Port mirroring  DHCP Client oraz Server  Jumbo frame  Broadcast storm control  Tablica ARP musi obsługiwać minimum 64 wpisy  Obsługa list ACL(Access Control Lists)  IEEE 802.1D  IEEE 802.1p  IEEE 802.1Q  IEEE 802.1ab  IEEE 802.1S  IEEE 802.1t  IEEE 802.1v  IEEE 802.1v  IEEE 802.1w  IEEE 802.1x  IEEE 802.2  IEEE 802.3  IEEE 802.3ab  IEEE 802.3ac  IEEE 802.3ad  IEEE 802.3ae  IEEE 802.3az  IEEE 802.3I  IEEE 802.3I  IEEE 802.3u  IEEE 802.3x  IEEE 802.3z  TFTP v2  SNTP  IGMP v1/v2/v3 snooping  SSHv2  SNMPv1/2/3  RADIUS Tunnel Authentication  RADIUS Tunnel Accounting  Radius Accounting  TACACS+  sFlow | | |
| **Funkcjonalności zarządzania** | Zarządzanie przez GUI oraz przez wiersz poleceń.  Oprogramowanie musi posiadać pulpit nawigacyjny informujący o alertach, ostatnio zarejestrowanych zdarzeniach, stanie portów oraz wizualizacji urządzenia w jednym miejscu.  Oprogramowanie musi wyświetlać informacje o danym porcie po wskazaniu kursorem, w skład wyświetlanych danych musi wchodzi:   * Numer portu * Status portu (up, inactive, error, disabled) * Typ Portu (np. 1GBase-T, 10GbE SFP+) * VLAN przypisany do portu * LAG które port jest członkiem * Profil Portu   Oprogramowanie musi pokazywać średni ruch dzienny.  Oprogramowanie musi pokazywać status urządzenia w tym temperatury, wentylatorów oraz zasilania.  Oprogramowania musi posiadać dwa tryby zapisu konfiguracji:   * Tymczasowy zapis po ponownym uruchomieniu zmiany są usuwane * Konfiguracja stała, utrzymuje się po ponownym uruchomieniu   Oprogramowanie musi umożliwiać pobranie oprogramowania z pamięci wewnętrznej, USB,HTTP oraz TFTP.  Oprogramowanie musi umożliwiać utworzenie kopi zapasowej konfiguracji przełącznika na pamięci wewnętrznej, USB,HTTP oraz TFTP.  Musi istnieć możliwość przechowywania dwóch obrazów oprogramowania systemowego w pamięci urządzenia w tym musi być możliwość zmiany aktywnego obrazu przez GUI | | |
| **Zasilanie** | Wbudowany zasilacz maksymalny pobór 62W. | | |
| **Głośność** | Maksymalna głośność urządzenia nie może przekraczać 58 dB w maksymalnej temperaturze 50°C | | |
| **Temperatura** | Zakres temperatur pracy ciągłej co najmniej 0 – 50 °C | | |
| **Chłodzenie** | Aktywne, przepływ powietrza z przodu do tyłu. | | |
| **Gwarancja producenta** | minimum 2 lata | | |

# UPS

|  |  |  |  |
| --- | --- | --- | --- |
| **UPS** | | **Ilość** | **1 szt.** |
| **Wymagane minimalne parametry techniczne** | | | |
| **Moc znamionowa** | 3000 VA / 2700W | | |
| **Napięcie wejściowe w trybie podstawowym** | 230V | | |
| **Czas podtrzymania** | 100% obciążenia minimum 30 minut  50% obciążenia minimum 1 godzinę | | |
| **Częstotliwość na wyjściu** | 50/60 Hz +/- 3 Hz Synchronicznie z siecią | | |
| **Topologia** | Line interactive | | |
| **Czas przełączenia zasilania** | 2-4 ms | | |
| **Typ akumulatora** | Bezobsługowy szczelny akumulator kwasowo-ołowiowy | | |
| **Typowy czas ładowania** | Maks. 3 godziny | | |
| **Złącza wyjściowe** | 8x IEC320 C13 10A  1x IEC320 C19 16A | | |
| **Alarmy dźwiękowe** | Alarm przy zasilaniu akumulatora: alarm przy bardzo niskim poziomie naładowania akumulatora: konfigurowalne opóźnienia | | |
| **Panel sterowania** | Przyciski sterownicze i informacyjny wyświetlacz lcd | | |
| **Wysokość** | Max 4U | | |
| **Komunikacja i zarządzanie** | Zainstalowany interfejs komunikacyjny posiadający port RJ45 oraz USB umożlwiający:   * Rejestracje zdarzeń * Planowane wyłączanie i ponowne uruchamianie * Zdalne restartowanie sprzętu * Dostęp przez przeglądarkę * Wielopoziomowy dostęp użytkowników * Zdalne zarządzanie za pośrednictwem protokołu Telnet lub SSH. * Aktualizacja oprogramowania firmware zasilacza UPS * Podłączenie czujnika temperatury lub czujnika temperatury i wilgotności | | |
| **Gwarancja** | 3 lata gwarancji na urządzenie i 2 lata na akumulatory | | |

# UPS Stacje robocze

|  |  |  |  |
| --- | --- | --- | --- |
| **UPS Stacje robocze** | | **Ilość** | **18 szt.** |
| **Wymagane minimalne parametry techniczne** | | | |
| **Moc znamionowa** | 800 VA / 500W | | |
| **Zakres napięcia wejściowego** | 190 - 258V ± 5 | | |
| **Czas podtrzymania** | 100% obciążenia minimum 4 minuty  50% obciążenia minimum 13 minut | | |
| **Czas przełączenia zasilania** | Max 6 ms | | |
| **Złącza wyjściowe** | 8x IEC320 C13 10A | | |
| **Zabezpieczenia** | Przeciwzwarciowe, przeciążeniowe | | |
| **Sygnalizacja** | Akustyczna, wyświetlacz lcd | | |
| **Komunikacja** | Port USB | | |
| **Gwarancja** | 2 lata gwarancji | | |

# Zestaw komputerowy

|  |  |  |  |
| --- | --- | --- | --- |
| **Jednostki robocze** | | **Ilość** | **23 szt.** |
| **Wymagane minimalne parametry techniczne** | | | |
| **Typ** | Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta. | | |
| **Zastosowanie** | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. | | |
| **Procesor** | Procesor dedykowany do pracy w komputerach stacjonarnych. Procesor osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 19500 pkt. według wyników opublikowanych na stronie <http://www.cpubenchmark.net/cpu_list.php>. | | |
| **Pamięć RAM** | 8GB DDR4 3200MHz. Możliwość rozbudowy do min 64GB, jeden slot DIMM wolny. | | |
| **Pamięć masowa** | Dysk M.2 SSD 512GB PCIe NVMe  Obudowa musi umożliwać montaż dodatkowego dysku 2.5” lub 3.5” | | |
| **Wydajność grafiki** | Zintegrowana z procesorem | | |
| **Wyposażenie multimedialne** | Karta dźwiękowa min. dwukanałowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik w obudowie komputera. Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie port combo. | | |
| **Obudowa** | Typu MiniTower z obsługą kart PCI Express wyłącznie o pełnym profilu. Umożliwiająca montaż 1 x dysku 3.5” lub 1 x dysku 2.5” wewnątrz obudowy. Napęd optyczny zamontowany w dedykowanej wnęce zewnętrznej 5.25” typu slim. Obudowa fabrycznie przystosowana do pracy w orientacji pionowej. Otwory wentylacyjne usytuowane wyłącznie na przednim oraz tylnym panelu obudowy. Suma wymiarów obudowy nieprzekraczająca 800 mm.  Zasilacz o mocy min. 180W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%, Zasilacz w oferowanym komputerze musi się znajdować na stronie <http://www.plugloadsolutions.com/80pluspowersupplies.aspx>, do oferty należy dołączyć wydruk potwierdzający spełnienie wymogu 80plus  Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych). Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych) oraz musi 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). Wbudowany wizualny system diagnostyczny oparty o sygnalizację LED np. włącznik POWER, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED (zmiana barw oraz miganie). System usytuowany na przednim panelu. System diagnostyczny musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię BIOS’u, awarię procesora. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS. | | |
| **Bezpieczeństwo** | Ukryty w laminacie płyty głównej układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. System zapewniający pełną funkcjonalność, a także zachowujący interfejs graficzny nawet w przypadku braku dysku twardego oraz jego uszkodzenia, nie wymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej.  Procedura POST traktowana jest jako oddzielna funkcjonalność. | | |
| **BIOS** | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, typowej prędkości zainstalowanego procesora, minimalnej i maksymalnej osiąganej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, wszystkich urządzeniach podpiętych do dostępnych na płycie głównej portów SATA, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio.  Do odczytu wskazanych informacji nie mogą być stosowane rozwiązania oparte o pamięć masową (wewnętrzną lub zewnętrzną), zaimplementowane poza systemem BIOS narzędzia, np. system diagnostyczny, dodatkowe oprogramowanie.  Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń, możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym zdefiniowanym haśle administratora. Użytkownik po wpisaniu swojego hasła jest wstanie zidentyfikować ustawienia BIOS. Możliwość ustawienia haseł użytkownika i administratora składających się z cyfr, małych liter, dużych liter oraz znaków specjalnych. Możliwość włączenia/wyłączenia kontrolera SATA (w tym w szczególności pojedynczo), Możliwość ustawienia portów USB w trybie „no BOOT” (podczas startu komputer nie wykrywa urządzeń bootujących typu USB). Możliwość wyłączania portów USB pojedynczo.  Możliwość dokonywania backup’u BIOS wraz z ustawieniami na dysku wewnętrznym.  Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot’owania które umożliwia m.in.: uruchamianie systemu zainstalowanego na dysku twardym, uruchamianie systemu z urządzeń zewnętrznych, uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, uruchomienie graficznego systemu diagnostycznego, wejście do BIOS, upgrade BIOS. | | |
| **Wirtualizacja** | Sprzętowe wsparcie technologi wirtualizacji realizowane łącznie w procesorze, chipsecie płyty główej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu). | | |
| **System operacyjny** | Microsoft Windows 10 Professional (64-bit) lub równoważny, fabrycznie preinstalowany przez Producenta oferowanego komputera.  Parametry równoważności:   1. System operacyjny dla komputerów przenośnych, z graficznym interfejsem użytkownika, 2. System ma udostępniać dwa rodzaje graficznego interfejsu użytkownika:    1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,    2. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych, 3. Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym Polskim i Angielskim, 4. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe, 5. Wbudowany system pomocy w języku polskim, 6. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim, 7. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne, 8. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego, 9. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego, 10. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; 11. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami, 12. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi), 13. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer, 14. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji, 15. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji, 16. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe, 17. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 18. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: i. poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,   Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.   1. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); 2. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; 3. Mechanizmy logowania do domeny w oparciu o:    1. Login i hasło,    2. Karty z certyfikatami (smartcard),    3. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 4. Mechanizmy wieloelementowego uwierzytelniania. 5. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu, 6. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec, 7. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; 8. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach, 9. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń, 10. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem 11. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika, 12. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB. 13. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych 14. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych. 15. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu. | | |
| **Certyfikaty i standardy** | Urządzenia wyprodukowane zgodnie z normą ISO 9001 oraz ISO 50001 – certyfikaty załączyć do oferty  Deklaracja zgodności CE (załączyć do oferty)  Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram. | | |
| **Wymagania dodatkowe** | Wbudowane porty:  1 x HDMI 1.4  1 x DisplayPort 1.4  8 portów USB wyprowadzonych na zewnątrz obudowy, w układzie:   * Panel przedni: 2 x USB 3.2 gen 1 Typu A oraz 2 x USB 2.0 * Panel tylny: 2 x USB 3.2 gen 1 Typu A oraz 2 x USB 2.0   1 x port audio typu combo (słuchawka/mikrofon) na przednim panelu panelu  1 x RJ – 45  Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich portów USB 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),  Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki, dedykowana dla danego urządzenia, wyposażona w: 1 x PCIe x16 Gen.3, 2 x PCIe x1, 2 x DIMM z obsługą do 64 GB DDR4 RAM, 3 x SATA w tym min. 2 szt SATA 3.0.  Jedno złącze M.2 dla dysków oraz złącze M.2 bezprzewodowej karty sieciowej.  Klawiatura USB w układzie polski programisty  Mysz optyczna USB  Nagrywarka DVD +/-RW o prędkości min. 8x | | |
| **Ergonomia** | Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 26 dB (załączyć oświadczenie producenta). | | |
| **Wsparcie techniczne 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 komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego). | | |
| **Warunki gwarancji** | 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)  3-letnia gwarancja producenta świadczona na miejscu u klienta,  Czas reakcji serwisu - do końca następnego dnia roboczego.  Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty.  Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta – wymagane dołączenie do oferty oświadczenia Producenta potwierdzonego, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta  W przypadku awarii dysk twardy zostaje u Zamawiającego – do oferty załączyć oświadczenie podmiotu realizującego serwis lub producenta o spełnieniu tego warunku | | |
| **Dodatkowe oprogramowanie** | Oprogramowanie producenta komputera z nieograniczoną czasowo licencją na użytkowanie umożliwiające:  - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,  - sprawdzenie przed zainstalowaniem wszystkich sterowników, aplikacji oraz BIOS bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem w celu uzyskania informacji o: poprawkach i usprawnieniach dotyczących aktualizacji, dacie wydania ostatniej aktualizacji, priorytecie aktualizacji, zgodności z systemami operacyjnymi  - dostęp do wykazu najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne  - włączenie/wyłączenie funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji  - sprawdzenie historii aktualizacji z informacją, jakie sterowniki były instalowane z dokładną datą i wersją (rewizja wydania)  - dostęp do wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu \*.xml  - dostęp do raportu uwzględniającego informacje o znalezionych, pobranych i zainstalowanych aktualizacjach z informacją, jakich komponentów dotyczyły, możliwość exportu takiego raportu do pliku \*.xml  Raport musi zawierać datę i godzinę podjętych i wykonanych akcji/zadań w przedziale czasowym min. 1 roku. | | |
| **Monitor** | | | |
| **Monitor** | | **Ilość** | **23 szt.** |
| **Wymagane minimalne parametry techniczne** | | | |
| **Typ panelu LCD** | IPS | | |
| **Rozmiar ekranu** | 23,8 cala | | |
| **Rozdzielczość** | 1920 x 1080 | | |
| **Czas reakcji** | Max. 4 ms | | |
| **Jasność** | Min. 250 cd/m² | | |
| **Kontrastu** | 1000:1 | | |
| **Wejścia** | VGA, DVI, HDMI | | |
| **Pochylenie** | -5/20 | | |
| **Certyfikaty** | Certyfikat TCO, RoHS | | |
| **Akcesoria** | W zestawie kabel HDMI, przewód zasilający | | |
| **Gwarancja** | Minimum 3 lata | | |

# Pakiet biurowy

|  |  |  |
| --- | --- | --- |
| **Pakiet biurowy** | **Ilość** | **17 szt.** |
| **Wymagane minimalne parametry techniczne** | | |
| **Microsoft Office 2021 Home & Business lub równoważny, spełniający kryteria równoważności:**   1. Wymagania odnośnie interfejsu użytkownika:    * + Pełna polska wersja językowa interfejsu użytkownika      + Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych      + Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się. 2. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:    * + posiada kompletny i publicznie dostępny opis formatu,      + ma zdefiniowany układ informacji w postaci XML zgodnie z Tabelą B1 załącznika   2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)   * + - umożliwia wykorzystanie schematów XML     - wspiera w swojej specyfikacji podpis elektroniczny zgodnie z Tabelą A.1.1 załącznika   2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych  (Dz.U.05.212.1766)   1. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców. 2. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy) 3. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim. 4. Pakiet zintegrowanych aplikacji biurowych musi zawierać:    * Edytor tekstów    * Arkusz kalkulacyjny    * Narzędzie do przygotowywania i prowadzenia prezentacji    * Narzędzie do tworzenia i wypełniania formularzy elektronicznych    * Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) 5. Edytor tekstów musi umożliwiać:    * Edycję i formatowanie tekstu w języku polskim, angielskim i niemieckim 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    * Sprawdzanie pisowni w języku polskim    * Śledzenie zmian wprowadzonych przez użytkowników    * 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    * Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003 lub Microsoft Word 2007, 2010, 2013 i 2016 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu    * Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji    * Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące   na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem.   * + Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze i pozwalające zapisać plik wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i Prawnych.  1. 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)    * 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    * Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą   oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007, 2010, 2013 i 2016, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń   * + Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji  1. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:    * Przygotowywanie prezentacji multimedialnych, które będą:   o Prezentowanie przy użyciu projektora multimedialnego o Drukowanie w formacie umożliwiającym robienie notatek o 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   + Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007, 2010, 2013 i 2016.   + Przesłanie danych przy użyciu usługi Web (tzw. web service).   + Wypełnianie formularza elektronicznego i zapisywanie powstałego w ten sposób dokumentu w pliku w formacie XML.   + Podpis elektroniczny formularza elektronicznego i dokumentu powstałego z jego wypełnienia.  1. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:    * Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego    * 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    * Zarządzanie kalendarzem    * Udostępnianie kalendarza innym użytkownikom    * 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 wirtualizacyjne

|  |  |  |
| --- | --- | --- |
| **Oprogramowanie wirtualizacyjne** | **Ilość** | **1 kpl.** |
| **Wymagane minimalne parametry techniczne** | | |
| Zamawiający wymaga dostarczenia oprogramowania wizualizacyjnego dla dostarczanego serwera. Dostarczane oprogramowanie wirtualizacje musi być objęte wsparciem technicznym dającym dostęp do repozytorium klasy Enterprise przez okres min. 5 lat.  Oferowane oprogramowanie musi wykorzystywać technologię wirtualizacji KVM i LXC.  Musi istnieć możliwość zarządzania z poziomu interfejsu web oraz CLI.  Interfejs zarządzania z poziomu przeglądarki musi być w języku polskim.  Oprogramowanie musi umożliwiać tworzenie klastrów wysokiej dostępności.  Oprogramowanie musi zapewniać obsługę sieciowych pamięci masowej:   * LVM Group (network backing with iSCSI targets) * iSCSI target * NFS Share * SMB/CIFS * Ceph RBD * Direct to iSCSI LUN * GlusterFS * CephFS   Oprogramowanie musi zapewniać obsługę lokalnych pamięci masowej:   * LVM Group * ZFS   Oferowane oprogramowanie musi posiadać interfejs webowy w języku polskim.  Oprogramowanie musi mieć wbudowane funkcjonalności: kopii zapasowej, zapory sieciowej, replikacji pamięci masowej.  Oprogramowanie musi umożliwiać tworzenie maszyn wirtualnych systemów Linux oraz Windows. | | |

# Laptop

|  |  |  |  |
| --- | --- | --- | --- |
| **Laptop** | | **Ilość** | **5 szt.** |
| **Wymagane minimalne parametry techniczne** | | | |
| **Zastosowanie** | Komputer mobilny będzie wykorzystywany dla potrzeb aplikacji biurowych, edukacyjnych, obliczeniowych, dostępu do Internetu oraz poczty elektronicznej. | | |
| **Matryca** | 15.6” FHD (1920 x 1080), powłoką przeciwodblaskową, jasność 250 nits, kontrast 700:1, NTSC 45% | | |
| **Wydajność** | Procesor osiągający w teście PassMark CPU Mark wynik min. 10 000 pkt według wyników opublikowanych na stronie http://www.cpubenchmark.net | | |
| **Pamięć RAM** | 8GB DDR4 3200MHz możliwość rozbudowy do min 32GB, 2 sloty na pamięci w tym min. jeden wolny | | |
| **Pamięć masowa** | 256GB SSD M.2 NVMe  Fabrycznie dostosowane miejsce do instalacji drugiego dysku M.2 | | |
| **Karta graficzna** | Zintegrowana z procesorem | | |
| **Multimedia** | Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki stereo o mocy 2x 2W.  Dwa kierunkowe, cyfrowe mikrofony z funkcją redukcji szumów i poprawy mowy wbudowane w obudowę matrycy.  Kamera internetowa z diodą informującą o aktywności, 0.9 Mpix, trwale zainstalowana w obudowie matrycy wyposażona w mechaniczną przysłonę.  czytnik kart micro SD, 1 port audio typu combo (słuchawki i mikrofon) | | |
| **Bateria i zasilanie** | Min. 63Whr umożliwiająca jej szybkie naładowanie do poziomu 35% w 20 minut, do 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin.  Zasilacz o mocy min. 65W TYP-C | | |
| **Waga i wymiary** | Waga max 1,85kg z baterią | | |
| **Obudowa** | Szkielet obudowy i zawiasy notebooka wzmacniane, dookoła matrycy uszczelnienie chroniące klawiaturę notebooka, po zamknięciu przed kurzem i wilgocią. Kąt otwarcia notebooka min 180 stopni.  Komputer spełniający normy MIL-STD-810H (załączyć oświadczenie producenta) | | |
| **BIOS** | BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, wymagana pełna obsługa za pomocą klawiatury i urządzenia wskazującego (wmontowanego na stałe) oraz samego urządzenia wskazującego. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji, oraz posiadać: datę produkcji komputera (data produkcji nieusuwalna), o kontrolerze audio, procesorze, a w szczególności min. i max. osiągana prędkość, pamięci RAM z informacją o taktowaniu i obsadzeniu w slotach. Niezmazywalne (nieedytowalne) pole asset tag z możliwością wpisywania min. znaków specjalnych. Funkcje logowania się do BIOS na podstawie hasła systemowego/użytkownika, administratora (hasła niezależne), Blokowanie hasłem systemowym/użytkownika dostępu do dysku twardego, funkcja umożliwiająca założenie hasła na dysk, informację o stanie naładowania baterii (stanu użycia), podpiętego zasilacza, zarządzanie trybem ładowania baterii (np. określenie docelowego poziomu naładowania). Możliwość nadania numeru inwentarzowego z poziomu BIOS bez wykorzystania dodatkowego oprogramowania, jak i konieczności aktualizacji BIOS.  Możliwość włączenia/wyłączenia funkcji automatycznego tworzenia recovery BIOS na dysku twardym. | | |
| **Certyfikaty** | Urządzenie musi być wyprodukowane zgodnie z normami ISO 9001, ISO 14001 oraz  ISO 50001 (certyfikaty zalączyć do oferty)  Deklaracja zgodności CE (załączyć do oferty)  Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki  Potwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym (wydruk ze strony) | | |
| **Diagnostyka** | System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. Działający w pełni, bez okrojonych funkcjonalności nawet w przypadku uszkodzonego dysku, braku dysku lub sformatowanym dysku, dostępu do sieci i internetu oraz bez konieczności podłączenia urządzeń wewnętrznych i zewnętrznych. | | |
| **Bezpieczeństwo** | Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu powoduje uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej.  Wbudowany czyjnik otwarcia dolnej pokrywy obudowy | | |
| **System operacyjny** | Microsoft Windows 10 Professional (64-bit) lub równoważny, fabrycznie preinstalowany przez Producenta oferowanego komputera.  Parametry równoważności:   1. System operacyjny dla komputerów przenośnych, z graficznym interfejsem użytkownika, 2. System ma udostępniać dwa rodzaje graficznego interfejsu użytkownika:    1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,    2. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych, 3. Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym Polskim i Angielskim, 4. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe, 5. Wbudowany system pomocy w języku polskim, 6. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim, 7. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne, 8. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego, 9. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego, 10. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; 11. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami, 12. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi), 13. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer, 14. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji, 15. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji, 16. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe, 17. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 18. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: i. poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,   Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.   1. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); 2. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; 3. Mechanizmy logowania do domeny w oparciu o:    1. Login i hasło,    2. Karty z certyfikatami (smartcard),    3. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 4. Mechanizmy wieloelementowego uwierzytelniania. 5. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu, 6. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec, 7. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; 8. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach, 9. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń, 10. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem 11. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika, 12. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB. 13. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych 14. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych. 15. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu. | | |
| **Oprogramowanie dodatkowe** | Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające :  - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, | | |
| **Wymagania dodatkowe** | Wbudowane porty i złącza: 1x HDMI 2.0, 1x RJ-45, 2x USB 3.2 w tym jeden port z zasilaniem, 2x Thunderbolt 4, złącze na linkę zabezpieczającą  Wydzieloną klawiaturą numeryczną i wbudowane w klawiaturze podświetleniem  Wszystkie klawisze funkcyjne typu : mute, regulacja głośności, print screen dostępne w ciągu klawiszy F1-F12.  Karta Wi-Fi 6 AX + Bluetooth 5.2 | | |
| **Warunki gwarancyjne, wsparcie techniczne** | 3-letnia gwarancja producenta świadczona na miejscu u klienta  Czas reakcji serwisu - do końca następnego dnia roboczego  Firma serwisująca musi posiadać ISO 9001: 2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty.  Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.  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) | | |

# Oprogramowanie biurowe

|  |  |  |
| --- | --- | --- |
| **Oprogramowanie biurowe** | **Ilość** | **5 szt.** |
| **Wymagane minimalne parametry techniczne** | | |
| Office 365 Business Standard na okres 2 lat lub równoważna licencja subskrypcyjna  Licencja subskrypcyjna na okres 2 lat musi zapewnić użytkownikom co najmniej:   * dostęp do wersji internetowych i mobilnych aplikacji pakietu biurowego w którego skład wchodzą:   a. Edytor tekstów;  b. Arkusz kalkulacyjny;  c. Narzędzie do przygotowywania i prowadzenia prezentacji;  d. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami  i zadaniami).   * zawsze aktualne wersje aplikacji dostępnych internetowo, * jednoczesną pracę wielu użytkownikom nad tym samym dokumentem w czasie rzeczywistym, * hosting poczty e-mail w skrzynce pocztowej o pojemności 50 GB, * pocztę e-mail klasy biznesowej na telefonach, tabletach, komputerach i w Internecie, * zarządzanie kalendarzem, udostępnianie wolnych terminów spotkań, plany spotkania i przypomnienia, * udostępnianie kalendarzy, * dodawanie nowych kont e-mail, usuwanie i przywracanie usuniętych kont e-mail, * przechowywanie i udostępnianie plików w magazynach chmurowych o pojemności 1 TB, * synchronizacja zapisanych plików w chmurze pomiędzy urządzeniami użytkownika, * zabezpieczenie i udzielanie uprawnień do poszczególnych plików, * organizowanie spotkań online i rozmów wideo z ponad 200 użytkownikami, * planowanie harmonogramów i dziennych zadań, * ochronę poczty e-mail przed spamem, złośliwym oprogramowaniem i znanymi zagrożeniami, * możliwość tworzenia grup zabezpieczeń i uprawnień dla określonych użytkowników, * tworzenie zasad dotyczących haseł, wymuszanie zmiany haseł po upływie określonej liczby dni, * dostęp do pomocy technicznej telefonicznie lub za pośrednictwem Internetu w dowolnym momencie * czas bezawaryjnej pracy na poziomie 99,9%. * klasyczną, instalowalną wersję aplikacji, aktualizowaną na bieżąco * system obsługi relacyjnych baz danych z obsługą baz danych typu MS Access, | | |

# Antywirus

|  |  |  |
| --- | --- | --- |
| **Antywirus** | **Ilość** | **5 szt.** |
| **Wymagane minimalne parametry techniczne** | | |
| 1. Rozwiązanie musi wspierać systemy operacyjne Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11.  2. Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows.  3. Rozwiązanie musi wspierać architekturę ARM64.  4. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.  5. Instalator rozwiązania musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.  6. Pomoc w rozwiązaniu (help) i dokumentacja rozwiązania dostępna co najmniej w języku polskim oraz angielskim.  7. Skuteczność rozwiązania potwierdzona nagrodami VB100 i AV-comparatives.    Ochrona antywirusowa i antyspyware  8. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.  9. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.  10. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami.  11. Rozwiązanie musi wykrywać potencjalnie niepożądane, niebezpieczne oraz podejrzane aplikacje.  12. Rozwiązanie musi posiadać możliwość skanowania w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.  13. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu.  14. Rozwiązanie musi posiadać możliwość definiowania zadań w harmonogramie, w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym, jeśli tak – nie wykonywało danego zadania.  15. Rozwiązanie musi posiadać możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).  16. Rozwiązanie musi posiadać opcję skanowania „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.  17. Rozwiązanie musi posiadać możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.  18. Rozwiązanie musi posiadać możliwość skanowania dysków sieciowych i dysków przenośnych.  19. Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych.  20. Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.  21. Administrator musi mieć możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.  22. Rozwiązanie musi posiadać możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.  23. Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji.  24. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera.  25. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.  26. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.  27. Rozwiązanie musi posiadać 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.  28. Rozwiązanie musi posiadać wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.  29. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.  30. Rozwiązanie musi umożliwiać 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).  31. Rozwiązanie musi automatycznie integrować skaner POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.  32. Rozwiązanie musi posiadać możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.  33. Rozwiązanie musi umożliwiać skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.  34. Rozwiązanie musi posiadać możliwość blokowania możliwości przeglądania wybranych stron internetowych. Rozwiązanie musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL.  35. Rozwiązanie musi posiadać możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora.  36. Rozwiązanie musi automatycznie integrować się z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.  37. Rozwiązanie musi umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.  38. Rozwiązanie musi zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe.  39. Rozwiązanie musi posiadać możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta.  40. Administrator ma mieć możliwość zdefiniowania portów TCP, na których rozwiązanie będzie realizowało proces skanowania ruchu szyfrowanego.  41. Rozwiązanie musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.  42. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym.  43. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.  44. W przypadku, gdy stacja robocza nie będzie posiadała dostępu do sieci Internet, ma odbywać się skanowanie wszystkich procesów, również tych, które wcześniej zostały uznane za bezpieczne.  45. Rozwiązanie musi posiadać dwa wbudowane niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.  46. Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.  47. Rozwiązanie musi posiadać możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.  48. Do wysłania próbki zagrożenia do laboratorium producenta, rozwiązanie nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika.  49. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.  50. Rozwiązanie musi posiadać możliwość zabezpieczenia konfiguracji hasłem, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie.  51. Rozwiązanie musi posiadać możliwość zabezpieczenia przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji rozwiązanie musi pytać o hasło.  52. Hasło do zabezpieczenia konfiguracji rozwiązania oraz deinstalacji musi być takie samo.  53. Rozwiązanie musi mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji.  54. Rozwiązanie musi mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.  55. Po instalacji rozwiązania, 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 zagrożeń.  56. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku.  57. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym.  58. Rozwiązanie musi posiadać umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.  59. Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia.  60. Rozwiązanie musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.  61. Rozwiązanie musi umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.  62. Rozwiązanie musi posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.  63. W momencie podłączenia zewnętrznego nośnika, rozwiązanie musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.  64. Administrator ma posiadać możliwość takiej konfiguracji rozwiązania, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.  65. Rozwiązanie musi być wyposażone w system zapobiegania włamaniom działający na hoście (HIPS).  66. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:  • tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,  • tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,  • tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,  • tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,  • tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.  67. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o:  aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.  68. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.  69. Rozwiązanie musi posiadać zaawansowany skaner pamięci.  70. Rozwiązanie musi być wyposażone w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.  71. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.  72. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.  73. Rozwiązanie musi posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie.  74. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.  75. Rozwiązanie musi posiadać możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.  76. Rozwiązanie musi posiadać możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego rozwiązanie zgłosi posiadanie nieaktualnego silnika detekcji.  77. Rozwiązanie musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.  78. Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.  79. Rozwiązanie musi być wyposażone w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).  80. Rozwiązanie musi być wyposażone tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).  81. Rozwiązanie musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.  82. W momencie wykrycia trybu pełnoekranowego, rozwiązanie ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań rozwiązania.  83. Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym.  84. Rozwiązanie musi być wyposażone w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, kontroli dostępu do urządzeń, skanowania oraz zdarzeń.  85. Rozwiązanie musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji.  86. Rozwiązanie musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline.  87. Rozwiązanie musi mieć możliwość podejrzenia informacji o licencji, która znajduje się w programie.  88. W rozwiązaniu musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji.  89. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień rozwiązania na stacji końcowej.  90. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostaną przywrócone dotychczasowe ustawienia.  91. Administrator ma możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny.  92. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika.  93. Rozwiązanie musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki.  94. Rozwiązanie musi posiadać możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych.  95. Rozwiązanie musi posiadać możliwość definiowana stanów rozwiązania, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji.  96. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.  97. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.  98. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.  99. Rozwiązanie musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup.  100. Administrator ma możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny.  101. Rozwiązanie musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść”.  102. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.  103. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.  104. Rozwiązanie musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.  105. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.  106. Rozwiązanie musi posiadać ochronę przed dołączeniem komputera do sieci botnet.  107. Rozwiązanie musi posiadać ochronę przed atakami Brute-Force, która zablokuje próbę siłowego dostania się do stacji roboczej za pomocą protokołu RDP i SMB.  108. Rozwiązanie musi posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.  109. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu.  110. Oferowane oprogramowanie musi zostać dostarczone z wsparciem aktualizacji na okres 2 lat. | | |