OPIS PRZEDMIOTU ZAMÓWIENIA

**INDEKS AL.**

**Komputer All-in-One – 10 szt.**

|  |  |  |
| --- | --- | --- |
| **Nazwa komponentu** | **Wymagania minimalne** | |
| **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. | |
| **Obudowa** | Typu All-in-One zintegrowana z monitorem min. 23.8”. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej, demontaż tylnej pokrywy musi odbywać się bez użycia narzędzi. Systemu montażowy VESA 100. Suma wymiarów obudowy bez zainstalowanego standu maks. 96cm. | |
| **Typowe parametry wyświetlacza** | Rozmiar i typ matrycy | 23,8” IPS lub WVA |
| Rozdzielczość | FHD (1920x1080) |
| Częstotliwość odświeżania | 100Hz |
| Jasność | 250 cd/m² |
| Kontrast | 1500:1 |
| Barwa koloru | 99% sRGB |
| Poziome kąty widzenia | 178 stopni |
| Rodzaj matrycy | Matowa IPS |
| **Płyta główna** | Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona logo producenta oferowanej jednostki, dedykowana dla danego urządzenia; wyposażona w min. 2 złącza SO - DIMM z obsługą do 64GB DDR5 pamięci RAM, min. 2 złącza M.2 dla dysku oraz 1 złącze M.2 karty WiFi. | |
| **Procesor** | Procesor osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik minimum 39000 pkt. według wyników opublikowanych na stronie <http://www.cpubenchmark.net/cpu_list.php>. | |
| **Pamięć RAM** | 16GB DDR5 5600 MT/s’ jeden slot pamięci wolny na dalszą rozbudowę | |
| **Pamięć masowa** | Dysk M.2 SSD 512GB PCIe NVMe | |
| **Karta graficzna** | Zintegrowana z procesorem | |
| **Komunikacja** | Karta sieciowa 10/100/1000 zintegrowana z płytą główną, wspierająca obsługęWoL (funkcja włączana przez użytkownika),  Karta Wi-Fi 6E AX z Bluetooth 5.3 | |
| **Wyposażenie multimedialne** | Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki o mocy 2W każdy.  Wbudowana w obudowę matrycy cyfrowa kamera Full HD mechanicznie chowana w obudowie (nie dopuszcza się kamer przekręcanych i wystających poza obrys obudowy).  Wbudowane w obudowę dwa mikrofony  Wbudowany w obudowę czytnik kart pamięci SD 4.0 (nie dopuszcza się stosowania zewnętrznych czytników USB); | |
| **Porty** | Porty wlutowane w płytę główną i wyprowadzone bezpośrednio bez stosowania przejściówek, adapterów, rozgałęziaczy itp.:  4 x USB 3.2 Gen 2 Typu A  2 x USB 3.2 Gen 1 Typu A  1 x USB 3.2 Gen 2x2 Typu C  1 x USB 3.2 Gen 2 Typu C  1 x Port Audio combo (słuchawki i mikrofon)  1 x DisplayPort 1.4a (wyjście wideo)  1 x HDMI 2.1 (wyjście wideo)  1 x HDMI 1.4b (wejście wideo); | |
| **Bezpieczeństwo** | Dedykowany układ sprzętowy TPM min. 2.0.  Komputer musi być wyposażony w czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym.  Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (wbudowane w obudowę gniazdo blokady Kensington) oraz kłódki (oczko w obudowie do założenia kłódki). | |
| **Ochrona oprogramowania układowego** | Komputer wyposażony w mechanizm weryfikacji i ochrony BIOS/UEFI, działający automatycznie przy każdym uruchomieniu komputera poza warstwą systemu operacyjnego oraz w samym środowisku systemu operacyjnego. Mechanizm musi umożliwiać ochronę oprogramowania układowego poprzez weryfikację integralności BIOS/UEFI pod kątem próby jego modyfikacji oraz ataku w trakcie rozruchu komputera (również podczas uruchamiania systemu operacyjnego). Weryfikacja poprawności BIOS/UEFI musi odbywać się poza hostem. | |
| **BIOS/UEFI** | Możliwość odczytania z BIOS informacji o:   * Wersji BIOS * Numerze seryjnym komputera * Numerze inwentarzowym * Typie (modelu) procesora, ilości rdzeni. * Zaimplementowanej sprzętowej technologii zdalnego zarządzania. * Ilości pamięci RAM, jej prędkości oraz obsadzeniu w slotach. * Pojemności i modelu zainstalowanego dysku. * MAC adresie zintegrowanej karty sieciowej   BIOS musi umożliwiać:   * Włączenie/wyłączenie zintegrowanej karty sieciowej * Włączenie/wyłączenie karty sieci bezprzewodowej oraz Bluetooth (o ile występuje) * Włączenie/wyłączenie karty audio * Włączenie/wyłączenie poszczególnych portów USB | |
| **BIOS/UEFI bezpieczeństwo** | W celu zapewnienia możliwie najwyższego poziomu bezpieczeństwa danych organizacji, BIOS/UEFI musi umożliwiać:   * Nadanie hasła administratora * Ustawienie hasła dla zainstalowanego dysku * Ustawienie portów USB w trybie „No BOOT” * Zarządzanie funkcją Wake on Lan oraz PXE Boot zintegrowanej karty sieciowej * Zarządzanie funkcją Secure Boot * Zarządzanie układem TPM * Zarządzania funkcją tworzenia recovery BIOS * Zarządzania funkcją downgrade BIOS. * Zarządzanie czujnikiem otwarcia obudowy * Zapisywanie incydentów w formacie tzw. logów z możliwością ich przejrzenia. * Bezpieczne usuwanie danych z zainstalowanego dysku zgodnie z wytycznymi NIST 800-88r1 * Nadanie numeru inwentarzowego bezpośrednio w BIOS bez użycia dodatkowego oprogramowania. Nadany numer nie może być edytowalny w BIOS ani nie może ulec skasowaniu po jego aktualizacji. * Możliwość nadania hasła uniemożliwiającego rozruch systemu operacyjnego, możliwość zmiany tego hasła w BIOS musi być zachowana także po nadaniu hasła administratora. * Możliwość blokowania upgrade BIOS przez system operacyjny. * Blokowanie downgrade BIOS w celu zapewnienia kompatybilności z poprawkami systemu operacyjnego. | |
| **Oprogramowanie diagnostyczne** | System diagnostyczny z graficznym interfejsem użytkownika, działający poza środowiskiem systemu operacyjnego, dostępny z poziomu BIOS lub szybkiego menu boot’owania.  System umożliwiający przetestowanie komponentów bez konieczności uruchamiania systemu operacyjnego. System musi posiadać wszystkie swoje funkcjonalności w przypadku: braku dysku, uszkodzenia dysku, sformatowania dysku, braku dostępu do sieci, internetu. Nie dopuszcza się stosowania wewnętrznych i zewnętrznych urządzeń w celu uzyskania funkcjonalności. Pełna obsługa systemu diagnostycznego za pomocą klawiatury i myszy jak i samej myszy. | |
| **Zintegrowany wizualny system diagnostyczny** | Wbudowany wizualny system diagnostyczny, zlokalizowany w obudowie lub w przycisku włączania, działający w oparciu sygnalizację LED, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami poprzez zmianę statusów wyświetlania diody (miganie w określonej sekwencji oraz zmiana barw wyświetlania).  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. | |
| **Zasilacz** | Zasilacz wewnętrzny o mocy nie większej niż 160W i sprawności na poziomie 85% przy 50% obciążenia.  Zasilacz w oferowanym komputerze musi się znajdować na stronie <https://www.clearesult.com/80plus/> lub jej podstronach. | |
| **Zdalne zarządzanie** | Wbudowana w płytę główną technologia zdalnego monitorowania i zarządzania komputerem na poziomie sprzętowym (out-of-band) działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC. Wymagana jest obsługa funkcji zdalnego zarządzania przez wbudowane w komputer porty zarówno sieci przewodowej LAN, jak i bezprzewodowej WLAN, z wykorzystaniem protokołów TCP/IP w tym IPv6 wraz z szyfracją komunikacji zarządzania z silnym protokołem minimum TLS 1.2 i zestawami silnych szyfrów TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384;TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 & TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 lub silniejszymi/nowocześniejszymi.  Technologia ta powinna być zgodna z otwartymi standardami DMTF WS-MAN 1.0.0 (<http://www.dmtf.org/standards/wsman> ) oraz DASH 1.2.0 (<http://www.dmtf.org/standards/mgmt/dash>) oraz  musi obsługiwać łącznie wszystkie następujące funkcje:   1. Zdalny odczyt konfiguracji komponentów komputera – model komputera i jego nr seryjny, model procesora, ilość, rodzaj i nr seryjne modułów pamięci RAM, model i nr seryjny dysku HDD/SSD, wersja BIOS FW płyty głównej, nr seryjny płyty głównej, dla laptopów model, znamionowa pojemność, numer seryjny i data produkcji baterii; 2. kontrolę stanu zasilania komputera pozwalającą na sprawdzenie aktualnego stanu zasilania komputera (stany ACPI S0/S3/S4/S5) oraz zdalne włączenie komputera ze stanu pełnego wyłączenia, hibernacji, uśpienia i tzw. Modern Standby (Connected Standby) oraz zdalne wyłączenie/reset bez udziału systemu operacyjnego; 3. zdalną konfigurację ustawień komputera przez interfejs BIOS setup w trybie graficznym lub tekstowym (ASCII). 4. zdalne przejęcie konsoli tekstowej systemu – tzw. Text Console Redirection lub Serial over LAN z możliwością jej wykorzystania do zdalnej zmiany ustawień BIOS Setup oraz odblokowania MS BitLocker Recovery. 5. zdalne przejęcie pełnej konsoli graficznej systemu tzw. KVM Redirection (Keyboard, Video, Mouse) na poziomie sprzętowym bez udziału systemu operacyjnego ani dodatkowych programów, również w przypadku braku lub uszkodzenia systemu operacyjnego do rozdzielczości 2560×1600 (WQXGA) włącznie zgodnie z profilem DSP1076 standardu DASH <https://www.dmtf.org/sites/default/files/standards/documents/DSP1076_1.0.1.pdf>   Funkcja przekierowania konsoli graficznej musi przechwytywać każdy rodzaj wyświetlanego na fizycznym lokalnym ekranie obrazu włącznie z procesem uruchamiania komputera (POST), odblokowania systemu szyfracji dysku, ładowania OS z dowolnego nośnika, zamykania OS oraz błędów ww. procesów: POST, ładowania OS (np. brak nośnika uruchamiającego, uszkodzenia OS BSOD (Blue Screen of Death) bez potrzeby modyfikacji tzw. loadera OS. | |
| **Wirtualizacja** | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu). | |
| **System operacyjny** | Zainstalowany system operacyjny Windows 11 Pro, klucz licencyjny musi być zapisany trwale w BIOS i umożliwiać reinstalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego. | |
| **Oprogramowanie biurowe** | Microsoft Office Home& Business 2024 PL lub równoważny | |
| **Certyfikaty i standardy** | Certyfikat ISO 9001 dla producenta komputera  Certyfikat ISO 14001 dla producenta komputera  Certyfikat ISO 50001 dla producenta komputera  Deklaracja zgodności CE  Certyfikat EPEAT Silver dla oferowanego modelu komputera, dla Polski lub kraju członkowskiego UE – na podstwie ze strony <https://www.epeat.net/search-computers-and-displays> | |
| **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 28dB na podstawie raport badawczy z testów przeprowadzonych przez niezależną akredytowaną jednostkę lub oświadczenia producenta urządzenia. | |
| **Wymagania dodatkowe** | Bezprzewodowy zestaw klawiatura w układzie polski programisty oraz mysz optyczna.  Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszczonym na obudowie, oraz musi być wpisany na stałe w BIOS.  Wraz z komputerem należy dostarczyć dedykowany przez producenta komputera podstawę, montowaną do jednostki w sposób niewymagający użycia jakichkolwiek narzędzi.  Podstawa jednostki typu All – in – One musi umożliwiać:  Regulację pochyłu pionowego w zakresie od -5 do 30 stopni.  Regulację wysokości w zakresie minimum 10 cm.  Ustawienie jednostki w trybie Pivot.  Obrót podstawy w lewą oraz prawą stronę. | |
| **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). | |
| **Warunki gwarancji** | Min. 24 miesięczna gwarancja producenta świadczona na miejscu u klienta wraz ze wsparciem technicznym dla fabrycznie zainstalowanych aplikacji.  Przyjmowanie zgłoszeń serwisowych w trybie 24/7/365 przez ogólnopolską linię telefoniczną oraz stronę internetową producenta  Czas reakcji serwisu - do końca następnego dnia roboczego  Firma serwisująca musi posiadać ISO 9001: 2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera .  W przypadku awarii dysk twardy zostaje u Zamawiającego – dokument potwierdzający spełnienie wymagania w postaci oświadczenia producenta  Zamawiający wymaga narzędzia do zarządzania zgłoszeniami serwisowymi samodzielnie przez portal internetowy lub inne narzędzie nie wymagające działań po stronie dostawcy. Narzędzie powinno umożliwiać:  - samodzielne wystawianie zgłoszeń serwisowych, śledzenie stanu zgłoszenia, komunikację z serwisem producenta przez edycję zlecenia i stanu zlecenia  - dostęp do materiałów serwisowych - co najmniej podręczników serwisowych i not serwisowych  - dostęp do materiałów szkoleniowych  - możliwości dodawania plików do otwieranego lub otwartego zlecenia (zdjęcia uszkodzeń, opisy etc.)  - śledzenie historii zleceń - raporty ze zleceń, historia - dla poszczególnych zleceń lub dla poszczególnych komputerów  - możliwość samodzielnego zarządzania wysyłką części (decyzja o zamówieniu części zamiennych i diagnostyka po stronie zamawiającego)  - możliwość rejestrowania i zarządzania zdarzeniami serwisowymi - agregowania zdarzeń z oprogramowania zarządzającego dostarczonego przez producenta, możliwość konwertowania zdarzeń na zgłoszenia serwisowe do producenta - z poziomu narzędzia.  - możliwość spięcia systemu serwisowego producenta z systemem helpdesk zamawiającego (dostępność API co najmniej dla opcji wystawienie zlecenia, sprawdzenie stanu zlecenia, raport zleceń) | |
| **Dodatkowe oprogramowanie** | Oprogramowanie zarządzające producenta komputera instalowane na etapie produkcji urządzenia, umożliwiające:  - monitorowanie komputera i generowanie zgłoszeń o błędach / nieprawidłowym działaniu w zakresie pracy komponentów i wydajności systemów  - powiadamiania o nowych wersjach sterowników i umożliwienie użytkownikowi wykonania upgrade systemu  - powiadamianie o problemach wydajnościowych i diagnozowanie / rozwiązywanie takich problemów  - śledzenie kluczowych komponentów i przewidywanie awarii przed ich wystąpieniem.  Dołączone do oferowanego komputera oprogramowanie z nieograniczoną licencją czasowo na użytkowanie umożliwiające:  - upgrade i instalacje wszystkich sterowników, dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,  - możliwość przed instalacją sprawdzenia każdego sterownika, BIOS’u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji:                  a. o poprawkach i usprawnieniach dotyczących aktualizacji                  b. dacie wydania ostatniej aktualizacji                  c. priorytecie aktualizacji                  d. zgodność z systemami operacyjnymi                  e. jakiego komponentu sprzętu dotyczy aktualizacja  - możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga.  - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr)  - sprawdzenia historii upgrade’u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania)  - dokładny wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu \*.xml  - raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach, zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku \*.xml. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.  Oprogramowanie umożliwiające aktualizację BIOS bezpośrednio z serwera producenta komputera przy wykorzystaniu bezpiecznego, szyfrowanego połączenia bez konieczności uruchamiania systemu operacyjnego oraz wykorzystywania zewnętrznych nośników pamięci masowej.  Oprogramowanie musi automatycznie rozpoznawać model urządzenia i bieżącą wersję BIOS. Oprogramowanie posiadające bezterminową licencję.  Możliwość zabezpieczenia dostępu do oprogramowania hasłem administratora.  Oprogramowanie umożliwiające przywrócenie obrazu systemu operacyjnego bezpośrednio z serwera producenta komputera przy wykorzystaniu bezpiecznego, szyfrowanego połączenia bez konieczności uruchamiania systemu operacyjnego.  W przypadku wystąpienia awarii oprogramowanie automatycznie uruchomi się i zapewni możliwość naprawy systemu operacyjnego lub przywrócenie go do stanu fabrycznego z możliwością dokonania kopii zapasowej plików przed uruchomieniem procesu.  Dodatkową funkcją oprogramowania jest możliwość wykonania kopii dysku (tzw. klonowania) wraz z plikami, ustawieniami aplikacji, systemem operacyjnym i jego ustawieniami.  Licencja pozwalająca na bezpłatne korzystanie z oprogramowania przez cały okres gwarancji komputera. | |

**Zasilacz awaryjny TYP 1 – 10 szt.**

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Moc pozorna/czynna | 350VA/245W |
| Liczba faz napięcia (wejście/wyjście) | 1/1 |
| Topologia | VI (line interactive) |
| Typ obudowy | Wolnostojąca/Tower |
| Zakres napięcia wejściowego | 191 ÷ 253 V ± 7 V |
| Zakres napięcia wyjściowego | 230 V AC ± 10 %. |
| Czas podtrzymania (100%/50%) | 2 min/9 min |
| Liczba akumulatorów wewnętrznych | 1 |
| Przyłącza wyjściowe | 1xIEC 320 C13 (10A), 2x PL |
| Sygnalizacja | Akustyczno- optyczna |
| Normy i deklaracje | PN-EN 62040-1:2009, CE |
| Gwarancja | min. 24 miesięczna gwarancja producenta na elektronikę i akumulatory |

**Serwer TYP 1 – 1 szt.**

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | * Obudowa Rack o wysokości max 1U * 8 slotów na dyski 2.5” * 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 jednego procesora. * Obsługa procesorów 144 rdzeniowych. * Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. * Na płycie głównej powinny znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. * Płyta główna powinna obsługiwać do 4TB pamięci RAM. |
| **Chipset** | * Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych. |
| **Procesor** | * Zainstalowany jeden procesor min. 12-rdzeniowy, min. 2.2GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 155 w teście SPECspeed®2017\_fp\_base, dostępnym na stronie www.spec.org dla konfiguracji jednoprocesorowej oferowanego serwera. |
| **RAM** | * 32GB DDR5 RDIMM 6400MT/s, |
| **Kontroler RAID** | * Sprzętowy kontroler dyskowy, posiadający   + Min. 8GB nieulotnej pamięci cache,   + Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.   + Wsparcie dla dysków samoszyfrujących   + Obsługa dysków 22.5 Gbps SAS, 12 Gbps SAS, and 6 Gbps SATA/SAS |
| **Dyski twarde** | * Zainstalowane:   + 4x dysk SAS o pojemności min. 2.4TB, Hot-Plug * Zainstalowane dwa dyski M.2 NVMe SSD o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. |
| **Gniazda PCI** | * Trzy sloty PCIe LP |
| **Interfejsy sieciowe/FC/SAS** | * 4 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) |
| **Wbudowane porty** | * 4 porty USB w tym min:   + 1 port USB 2.0 Type-C   + 2 porty USB 3.1   + 1 port USB 3.0 wewnątrz obudowy * Port VGA z tyłu obudowy |
| **Video** | * Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |
| **Zasilacze** | * Redundantne, Hot-Plug min. 800W klasy Titanium |
| **Elementy montażowe** | * Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych * Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych |
| **System operacyjny/dodatkowe oprogramowanie** | * Windows Server 2025 Standard * 10x Windows Server 2025/2022 Device CALs |
| **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. * 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 * Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). |
| **Karta Zarządzania** | * Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:   + zdalny dostęp do graficznego interfejsu Web karty zarządzającej   + 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 SNMP; IPMI2.0, VLAN tagging, SSH   + 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 sześciu administratorów jednocześnie   + Wsparcie dla automatycznej rejestracji DNS   + wsparcie dla LLDP   + wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej   + możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy.   + Monitorowanie zużycia dysków SSD   + Automatyczne zgłaszanie alertów do centrum serwisowego producenta   + Automatyczne update firmware dla wszystkich komponentów serwera   + Możliwość przywrócenia poprzednich wersji firmware   + Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON   + Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych   + Automatyczne tworzenie kopii ustawień serwera w opraciu o harmonogram.   + Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera   + kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania   + możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień   + możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera   + możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer   + możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe   możliwość rozszerzenia funkcjonalności o:   * + możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych narzędzi analitycznych jak Splunk, Grafana, ElasticSearch   + możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej   + Automatyczne odświeżanie certyfikatów SSL   + monitorowanie przepływu powietrza na bieżąco (w CFM) |
| **Oprogramowanie do zarządzania** | * Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:   + Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych   + integracja z Active Directory   + Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta   + Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish   + Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram   + Szczegółowy opis wykrytych systemów oraz ich komponentów   + Możliwość eksportu raportu do CSV, HTML, XLS, PDF   + Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.   + Grupowanie urządzeń w oparciu o kryteria użytkownika   + Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji   + Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach   + Szybki podgląd stanu środowiska   + Podsumowanie stanu dla każdego urządzenia   + Szczegółowy status urządzenia/elementu/komponentu   + Generowanie alertów przy zmianie stanu urządzenia.   + Filtry raportów umożliwiające podgląd najważniejszych zdarzeń   + Integracja z service desk producenta dostarczonej platformy sprzętowej   + Możliwość przejęcia zdalnego pulpitu   + Możliwość podmontowania wirtualnego napędu   + Kreator umożliwiający dostosowanie akcji dla wybranych alertów   + Możliwość importu plików MIB   + Przesyłanie alertów „as-is” do innych konsol firm trzecich   + Możliwość definiowania ról administratorów   + Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów   + Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)   + Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta   + Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów   + Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.   + Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.   + Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile   + Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.   + Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.   + Zdalne uruchamianie diagnostyki serwera.   + Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.   + Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.   + Integracja z środowiskiem VMware vCenter pozwalająca z konsoli/plugin:     - wykonać zautomatyzowaną aktualizację firmware serwerów w klastrze  Vmware do zdefiniowanej polityki poziomu mikrokodów     - wykonać/zweryfikować konfigurację serwera zgodną ze zdefiniowaną polityka konfiguracji     - z konsoli vCenter uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny)     - inwentaryzacja komponentów w serwerze i ich mikrokodów     - historia poboru mocy i temperatury serwera     - zbieranie danych diagnostycznych serwera do paczki serwisowej |
| **Oprogramowanie do monitorowania** | Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:   * Monitoring:   + ilość podłączonych oraz rozłączonych systemów   + stan podłączonych urządzeń   + informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów   + Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia   + informacje o statusie gwarancji dla poszczególnych urządzeń   + informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń   + informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych.   + Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych   + Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych.   + Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych.   + Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC.   + Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej.   + Monitoring parametrów serwerów z informacją o minimum:     - Obciążeniu procesora     - Zużyciu pamięci RAM     - Temperaturze procesorów     - Temperaturze powietrza wlotowego     - Zużyciu prądu     - Zmianach w fizycznej konfiguracji serwera     - Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.   + Monitoring parametrów pamięci masowych z informacją o minimum:     - Opóźnieniach     - IOPS     - Przepustowości     - Utylizacji kontrolerów     - Pojemność całkowita i dostępna     - Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów.     - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.     - Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata     - Informacje o poziomie redukcji danych     - Informacje o statusie replikacji oraz snapshotów   + Monitoring parametrów przełączników sieciowych z informacją o minimum:     - Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny     - Stanie komponentów: zasilacze, wentylatory     - Podłączonych hostach     - Ilości i statusu portów     - Utylizacji procesora     - Utylizacji poszczególnych portów     - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. * Aktualizacja firmware   + możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania * Raporty   + Możliwość generowania raportów dla serwerów zawierających informację o:     - Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej     - Średnim obciążeniu: procesorów, pamięci RAM, IO,   + Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o:     - Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji   + Generowanie raportów do plików CSV i PDF * Cyberbezpieczeństwo   + Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia.   + Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń.   + Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.   + Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. * Wspierane urządzenia   + Urządzenie Producenta dostarczane w ramach postępowania   + Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) * Wirtualny asystent   + Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; * Możliwość rozszerzenia funkcjonalności   + Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. * Inne   + Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android |
| **Certyfikaty** | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 * Serwer musi posiadać deklaracja CE. * Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej [www.epeat.net](http://www.epeat.net) potwierdzający spełnienie normy co najmniej Epeat Silver, dla kraju, w którym produkt będzie użytkowany, według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.** * Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025. |
| **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. |
| **Warunki gwarancji** | * Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. * Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. * Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. * Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. * Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. * Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. * Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:   + Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.   + Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.   + Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.   + Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.   + Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. * Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń . |
| **Dodatkowo** | * Zamawiający zaleca wykonawcom, aby w ramach oferowanych serwerów zapewnić pełne wsparcie dla następujących rozwiązań: Integrated Dell Remote Access Controller (iDRAC), Dell OpenManage Enterprise oraz Dell AIOps. Wsparcie dla wskazanych narzędzi jest istotne z uwagi na konieczność zapewnienia spójnego, centralnego zarządzania oraz monitorowania rozbudowywanej infrastrukturzy serwerowej, w szczególności w zakresie zdalnej administracji, automatyzacji zadań utrzymaniowych, monitoringu stanu urządzeń oraz proaktywnej analizy zdarzeń i anomalii. Zastosowanie tych rozwiązań pozwala na efektywne włączenie nowych serwerów w istniejące środowisko, zwiększenie dostępności usług, skrócenie czasu reakcji na incydenty oraz ograniczenie kosztów operacyjnych związanych z utrzymaniem infrastruktury. |

**Wymagania w zakresie instalacji i wdrożenia serwera:**

1. Instalacji serwera we wskazanej serwerowni i szafie rack
2. Instalacji systemu operacyjnego na posiadanych przez Zamawiającego
3. Instalacja i konfiguracja dwóch maszyn wirtualnych na oferowanym serwerze

**Zasilacz awaryjny TYP 2 – 1 szt.**

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalna** |
| Moc pozorna | 6000 VA |
| Moc rzeczywista | 6000 W |
| Liczba faz napięcia (wejście/wyjście) | 1/1 |
| Sprawność max (dla VFI) | 95% |
| Topologia | on-line (VFI), podwójna konwersja |
| Typ obudowy | Rack/Tower |
| Chłodzenie | Wymuszone, wewnętrzne wentylatory |
| Zakres napięcia wejściowego | 110 ÷ 275 V AC ± 3% |
| Kształt napięcia wyjściowego | sinusoidalny |
| Czas przełączania na pracę rezerwową | 0 ms |
| Czas podtrzymania UPS + 1 szt. Modułu Bateryjnego dla obciążenia (100%/80%/50%) | Min. 6/9/15 min |
| Zabezpieczenie przeciwzwarciowe gniazd wyjściowych | Bezpiecznik 20A |
| Zabezpieczenie przeciążeniowe | elektroniczne |
| Liczba akumulatorów wewnętrznych | Brak |
| Akumulatory w Modułach Bateryjnych | minimum 20x 12V 9Ah; szczelne, bezobsługowe |
| Maksymalna ilość modułów bateryjnych | 6 szt. |
| Ilość i typ gniazd wyjściowych | Minimum 2x IEC 320 C13 (10 A) + listwa zaciskowa + dodatkowy moduł PDU wyposażony w minimum 2x IEC 320 C13 (10 A) + 1x IEC 320 C19 (16A) niesterowalne oraz 2x IEC 320 C13 (10 A) + 1x IEC 320 C19 (16A) sterowalne |
| Interfejs komunikacyjny | RS232, USB HID, karta SNMP/http - wymagana na wyposażeniu |
| Sygnalizacja | Wyświetlacz LCD (informacje wskazujące pracę sieciową, bateryjną, przeciążenie i ładowanie akumulatora).  Diody LED |
| Oprogramowanie | oprogramowanie tego samego producenta co UPS, w języku polskim do zarządzania i monitorowania pracy UPS dla Windows, Linux oraz systemów wirtualizacji VMware, Hyper-V, Citrix XenServer bez ograniczeń co do ilości monitorowanych stanowisk (bez dodatkowych opłat za licencje)  możliwość edycji nazw urządzeń na liście monitorowanych UPSów |
| Normy i deklaracje | Certyfikat producenta: ISO 9001:2015  Potwierdzenie w zakresie prowadzenia serwisu ze strony producenta bądź udzielonej autoryzacji. Wymagane także potwierdzenie lokalizacji serwisu na terenie Polski. |
| Gwarancja | min. 24 miesiące gwarancji producenta na elektronikę i akumulatory |
| Serwis | autoryzowany serwis producenta zlokalizowany w Polsce.  serwis realizowany w systemie door to door  wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów w okresie gwarancji. |

**Przełącznik sieciowy – 1 szt.**

Wymaga się aby urządzenie posiadało następujące porty, protokoły oraz spełniało następujące funkcje:

* Ilość portów: 48 PoE+ 1GBASE-T, 4 x SFP+
* Tablica MAC min. 16K
* CPU klasy min. Quad-Core Cortex-A57 ARMv8 1.8Ghz
* Min. 2GB RAM
* Bufor 32Mb
* MTBF min. 620 000 godzin
* Wydajność min. 130,94 Mp/s
* Przepustowość min. 176 Gb/s
* Port USB Type-C
* Port zarządzania Out-of-band oraz konsolowy RJ45
* Web GUI
* Interfejs web umożliwiający automatyczne przypisanie konfiguracji do portów właściwej dla protokołów czy też producenta: NVX, AMX, NDI, ZeeVee, Aurora, Kramer, LibAV, Dante Video, SDVoE, AES67, Q-SYS, Audio Dante, AVB, Crestron DigitalMedia AV, NUCLEUS Converged AV, Shure, Sonos, Visionary AV
* Wymaga się aby powyższe szablony konfiguracji były stworzone przez producenta przełącznika a interfejs web w sposób jednoznaczny wskazywał że dany producent AV czy protokół jest obsługiwany przez dany szablon.
* Wymaga się aby interfejs web miał możliwość wykonywania poleceń tekstowych CLI bez potrzeby tworzenia oddzielnego połączenia Telnet lub SSH.
* Wymaga się aby w sposób manualny istniała możliwość wyboru trybu wykrywania urządzeń PoE. Jednym z takich trybów powinien być: 4ptdot3af
* HTTPs
* SSH
* Obsługa PTPv2
* STP, MTP, RSTP PV(R)STP
* IPv4/IPv6:
* PIM-SM
* PIM-DM
* SSM
* Obsługa IEEE 802.1AS-2011 gPTP, IEEE 802.1Qav-2009 FQTSS, IEEE 802.1Qat-2010 MSRP, IEEE 802.1ak MMRP, IEEE 802.1ak MVRP
* Kształtowanie ruchu na wejściu oraz wyjściu co 1 Kbps
* Radius
* TACACS+
* IGMPv1,v2 Querier
* CE: EN 55032:2012+AC:2013/CISPR 32:2012, EN 61000-3-2:2014,
* Class A, EN 61000-3-3:2013, EN 55024:2010
* VCCI : VCCI-CISPR 32:2016, Class A
* RCM: AS/NZS CISPR 32:2013 Class A
* CCC: GB4943.1-2011; YD/T993-1998; GB/T9254-2008 (Class A)
* FCC: 47 CFR FCC Part 15, Class A, ANSI C63.4:2014

Gwarancja: Wymaga się aby urządzenie było objęte gwarancją producenta w okresie min. 24 miesięcy realizowaną w systemie door-to-door przez serwis producenta. Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji.

**Serwer TYP 2 – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagania minimalne** |
| Typ | Sieciowy serwer plików NAS |
| Obudowa | Rack 1U |
| Procesor | 4-rdzeniowy procesor Intel® Celeron® N5095 o taktowaniu zwiększanym do 2,9 GHz |
| Pamięć RAM | 8 GB RAM |
| Wewnętrzna pamięć masowa | Możliwość instalacji 4 dysków 3,5-calowych SATA 6 Gb/s  Zainstalowane min. 2 dyski 3.5” 2TB SATA każdy |
| Kompatybilność dysków | Dyski twarde SATA 3,5-calowe Dyski SSD SATA 2,5-calowe |
| Interfejsy sieciowe | Min. 2 x 2,5 Gigabit Ethernet (2,5G/1G/100M/10M) |
| Złącza dodatkowe | Min. 2 porty typu A USB 3.2, 1x HDMI 1.4 |
| PCI slot | 1x PCIe Gen 3 x2 |
| Szyfrowanie | AES-NI |
| Zasilacz | 250W, 100–240 V |
| Certyfikaty | ISO 9001 |
| Gwarancja | Minimum 24 miesiące gwarancji |
| Dokumentacja użytkownika | Zamawiający wymaga dokumentacji w języku polskim lub angielskim, w formie elektronicznej. |

**Monitor 40” – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagania minimalne** |
| Typ | Sieciowy serwer plików NAS |
| Rozmiar ekranu: | 40 " / 101 cm |
| Rozdzielczość | Full HD / 1920 x 1080 |
| Częstotliwość odświeżania obrazu | Do 60 Hz |
| Technologia obrazu: | QLED |
| Podświetlenie matrycy: | Direct LED |
| Tuner | DVB-T2 (HEVC), DVB-S2, DVB-C, analogowy |
| Wbudowane głośniki | Tak min 16 W |
| Złącza | 2 (2x HDMI 1.4), USB min 1, |

**UTM – 1 szt.**

Wymagania ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu.

System wspiera protokoły 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 – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:

* 4 portami Gigabit Ethernet RJ-45.

1. System Firewall posiada wbudowany port konsoli szeregowej.
2. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall’a obsługa nie mniej niż 500 tys. jednoczesnych połączeń oraz 25 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 4 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 800 Mbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 3 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 750 Mbps.
6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 450 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
11. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.
12. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje 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.

1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.
3. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
4. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
5. Element systemu realizujący funkcję Firewall integruje 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.
* Cisco ACI.
* Google Cloud Platform (GCP).
* OpenStack.
* VMware NSX.
* Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:

* Wsparcie dla IKE v1 oraz v2.
* Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19, 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
* 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.
* Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
* Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
* Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
* Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.

1. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej.
8. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
9. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 18000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 5000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 260 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia 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. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego.
2. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
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 mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

 Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.

Gwarancja oraz wsparcie

System jest objęty serwisem gwarancyjnym producenta przez okres min. 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię.

Wymagania ogólne

1. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

**Wymagania w zakresie instalacji i wdrożenia urządzenia klasy UTM:**

Zamawiający wymaga:

1. Instalacji urządzenia klasy UTM we wskazanym punkcie dystrybucji okablowania.
2. Wdrożenia urządzenia klasy UTM do ochrony styku z Internetem we wskazanych przez Zamawiającego segmentach sieci, w tym:
   1. Konfiguracji interfejsów urządzenia (w tym LACP, VLAN),
   2. Konfiguracji routingu IP,
   3. Konfiguracji mechanizmów zarządzania,
   4. Konfiguracji reguł firewalla,
   5. Konfiguracji modułów funkcyjnych (min. IPS, AntiVirus).

**Oprogramowanie antywirusowe – 1 kpl.**

Wymagane dostarczenie licencji na 11 stanowisk PC i 2 serwery na okres min. 36 miesiące

**Administracja zdalna w chmurze**

1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

**Ochrona stacji roboczych – Windows**

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5. Rozwiązanie musi posiadać funkcjonalność przywrócenie plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware.
6. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
7. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
8. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
9. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
11. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
12. Rozwiązanie musi zapewniać 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).
13. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
14. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
15. Rozwiązanie musi zapewniać 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.
16. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
17. 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.

1. 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.
2. 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.
3. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
4. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
5. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
6. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
7. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:

* tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
* tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
* tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
* tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.

1. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
2. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
3. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
4. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
5. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
6. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
7. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

**Ochrona stacji roboczych – macOS**

1. Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 11 (Big Sur) lub nowszych.
2. Rozwiązanie musi wspierać architekturę Apple Silicon (ARM)
3. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.
4. Pomoc w rozwiązaniu (help) musi być dostępna co najmniej w języku polskim oraz angielskim.
5. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
6. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
7. Rozwiązanie musi posiadać funkcjonalność, która w momencie wykrycia trybu pełnoekranowego ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań.
8. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
9. Rozwiązanie musi posiadać możliwość zdalnego zarządzania z poziomu Administracji zdalnej.
10. 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).
    1. **Ochrona stacji roboczych – Linux**
11. Rozwiązanie musi wspierać systemy operacyjne Ubuntu Desktop, Red Hat Enterprise Linux oraz Linux Mint.
12. Rozwiązanie musi posiadać wsparcie dla dystrybucji 64-bitowych.
13. Pomoc (help) musi być dostępna co najmniej w języku polskim oraz angielskim.
14. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
15. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
16. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami.
17. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
18. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
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.

**Ochrona serwera**

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:

1. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
2. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
3. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
4. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
5. Rozwiązanie musi zapewniać 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.
6. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
7. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych*.*
8. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
9. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
2. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
3. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
4. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

**Szyfrowanie**

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
5. Rozwiązanie musi umożliwiać zalogowanie się do systemu przy pomocy metody jednokrotnego logowania (SSO).

**Ochrona urządzeń mobilnych opartych o system Android**

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
   1. usunięcie zawartości urządzenia,
   2. przywrócenie urządzenie do ustawień fabrycznych,
   3. zablokowania urządzenia,
   4. uruchomienie sygnału dźwiękowego,
   5. lokalizację GPS.
6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
   1. nazwę aplikacji,
   2. nazwę pakietu,
   3. kategorię sklepu Google Play,
   4. uprawnienia aplikacji,
   5. pochodzenie aplikacji z nieznanego źródła.

**Sandbox w chmurze**

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.
8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.
12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
13. Czysty,
14. Podejrzany,
15. Bardzo podejrzany,
16. Szkodliwy.
17. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
18. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
19. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

**INDEKS 29**

**Notebook – 1 szt.**

|  |  |
| --- | --- |
| Nazwa | Wymagane parametry techniczne |
| Zastosowanie | Komputer mobilny będzie wykorzystywany dla potrzeb aplikacji biurowych, edukacyjnych, obliczeniowych, dostępu do Internetu oraz poczty elektronicznej. |
| Matryca | 14” FHD+ (1920 x 1200), matryca IPS, powłoka przeciwodblaskowa, jasność 300 cd/m2, kontrast typowy 600:1, pokrycie barw 45% NTSC |
| Procesor | Procesor musi być wyposażony w jednostki przetwarzania neuronowego (NPU) o wydajności co najmniej 12 TOPS.  Procesor musi osiągać w teście PassMark Performance Test, co najmniej 17000 punktów w kategorii Average CPU Mark. Wynik dostępny na stronie: <https://www.cpubenchmark.net/cpu_list.php> |
| Pamięć RAM | Min. 16GB DDR5. Możliwość rozbudowy do co najmniej 64GB. Jeden slot na pamięć musi pozostać wolny. |
| Pamięć masowa | 512GB NVMe SSD M.2 |
| Karta graficzna | Zintegrowana karta graficzna. |
| Klawiatura i urządzenie wskazujące | Klawiatura z wbudowanym podświetleniem w układzie US – QWERTY.  Wszystkie klawisze funkcyjne typu: mute, mikrofon, regulacja głośności, print screen dostępne w ciągu klawiszy F1-F12. Dedykowany klawisz do obsługi asystenta AI.  Touchpad lub clickpad z obsługą gestów, umożliwiający kontrolowanie kursora na ekranie w systemie diagnostycznym oraz podczas instalacji systemu operacyjnego. |
| Multimedia | Wbudowane dwa głośniki o mocy 2W każdy.  Dwa kierunkowe, cyfrowe mikrofony z funkcją redukcji szumów i poprawy mowy.  Kamera internetowa FHD RGB 2 MPIX, trwale zainstalowana w obudowie matrycy opatrzona we wbudowaną mechaniczną przysłonę. |
| Łączność bezprzewodowa | Karta Wi-Fi 7 BE z Bluetooth 5.4 |
| Bateria i zasilanie | Bateria o pojemności min. 55WH.  Ładowanie baterii do poziomu 80% w czasie 1 godziny.  Zasilacz o mocy min. 60W ze złączem Typu – C |
| Waga | Katalogowa waga startowa nie większa niż 1.55kg wg. oficjalnej dokumentacji producenta. |
| Obudowa | Obudowa wykonana z aluminium (min. pokrywa matrycy oraz podpórka pod nadgarstki)  Kąt otwarcia notebooka min 180 stopni.  Komputer spełniający normy MIL-STD-810H. |
| Ochrona oprogramowania układowego | Komputer wyposażony w mechanizm weryfikacji i ochrony BIOS/UEFI, działający automatycznie przy każdym uruchomieniu komputera poza warstwą systemu operacyjnego oraz w samym środowisku systemu operacyjnego. Mechanizm musi umożliwiać ochronę oprogramowania układowego poprzez weryfikację integralności BIOS/UEFI pod kątem próby jego modyfikacji oraz ataku w trakcie rozruchu komputera (również podczas uruchamiania systemu operacyjnego). Weryfikacja poprawności BIOS/UEFI musi odbywać się poza hostem. |
| BIOS/UEFI | Możliwość odczytania z BIOS informacji o:   * Wersji BIOS * Numerze seryjnym komputera * Numerze inwentarzowym * Typie (modelu) procesora, ilości rdzeni, w * Zaimplementowanej sprzętowej technologii zdalnego zarządzania. * Ilości pamięci RAM i jej prędkości. * Pojemności i modelu zainstalowanego dysku. * MAC adresie zintegrowanej karty sieciowej lub adresie MAC Address Pass Through (tzw. MAPT); * Mocy podpiętego zasilacza * Poziomie naładowania baterii * Dacie produkcji komputera * Maksymalnej prędkości procesora * Kontrolerze audio (producent lub oznaczenie)   BIOS musi zapewniać możliwość zarządzania:   * Kamerą * Mikrofonem oraz głośnikami * Portami USB * Kontrolerem NVMe * Zintegrowaną kartą sieciową (o ile występuje) * Kartą sieci bezprzewodowej i bluetooth (o ile występuje) * Modemem WWAN (o ile występuje) * Podświetleniem klawiatury * Jasnością matrycy oddzielnie dla zasilania bateryjnego i sieciowego. * Trybami ładowania baterii w min. 4 predefiniowanych trybach. * Zarządzanie funkcją Power Delivery dla portu typu – C * Trybem pracy układu chłodzenia wg. Min. trzech predefiniowanych scenariuszu (zoptymalizowany, cicha praca, maksymalna wydajność) * Funkcją odpowiedzialną za zarządzanie podświetleniem klawiatury umożliwiająca wybór predefiniowanego trybu podświetlenia wg. sposobu lub czasu lub stopnia podświetlenia   Powyższa funkcjonalność musi być realizowana wyłącznie przez BIOS. Nie dopuszcza sie realizacji poprzez dodatkowe oprogramowanie oraz przez system diagnostyczny. |
| BIOS/UEFI - bezpieczeństwo | W celu zapewnienia możliwie najwyższego poziomu bezpieczeństwa danych organizacji, BIOS/UEFI musi umożliwiać:   * Nadanie hasła administratora * Ustawienie hasła dla zainstalowanego dysku * Ustawienie portów USB wtrybie „No BOOT” * Zarządzanie funkcją Wake on Lan oraz PXE Boot zintegrowanej karty sieciowej (o ile występuje) * Zarządzanie funkcją Secure Boot * Zarządzanie układem TPM * Zarządzania funkcją tworzenia recovery BIOS * Zarządzania funkcją downgrade BIOS. * Zarządzanie czujnikiem otwarcia obudowy (dolnej pokrywy). * Zapisywanie incydentów w formacie tzw. logów z możliwością ich przejrzenia. * Bezpieczne usuwanie danych z zainstalowanego dysku zgodnie z wytycznymi NIST 800-88r1 * Nadanie numeru inwentarzowego bezpośrednio w BIOS bez użycia dodatkowego oprogramowania. Nadany numer nie może być edytowalny w BIOS ani nie może ulec skasowaniu po jego aktualizacji. * Możliwość nadania hasła uniemożliwiającego rozruch systemu operacyjnego, możliwość zmiany tego hasła w BIOS musi być zachowana także po nadaniu hasła administratora. * Możliwość blokowania upgrade BIOS przez system operacyjny. * Blokowanie downgrade BIOS w celu zapewnienia kompatybilności z poprawkami systemu operacyjnego.   Powyższa funkcjonalność musi być realizowana wyłącznie przez BIOS. Nie dopuszcza sie realizacji poprzez dodatkowe oprogramowanie oraz przez system diagnostyczny. |
| Certyfikaty | Certyfikat ISO 9001 dla producenta sprzętu  Certyfikat ISO 14001 dla producenta sprzętu  Certyfikat ISO 50001 dla producenta sprzętu  Certyfikat EPEAT Gold, dla oferowanego modelu komputera. Wymagana certyfikacja na stronie: <https://www.epeat.net/search-computers-and-displays>  Deklaracja zgodności CE  Certyfikaty ISO oraz deklaracja zgodności muszą być wystawione dla tego samego producenta sprzętu. Za producenta uznaje się każda osobę fizyczną lub prawną albo jednostkę organizacyjną nie posiadającą osobowości prawnej dla której ten wyrób zaprojektowano lub wytworzono, w celu wprowadzenia go do obrotu lub oddania do użytku pod własną nazwą lub znakiem. Certyfikaty ISO winny być możliwe do obejrzenia/pobrania z oficjalnych stron www producenta sprzętu. |
| 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 25dB. |
| Oprogramowanie diagnostyczne | System diagnostyczny z graficznym interfejsem użytkownika, działający poza środowiskiem systemu operacyjnego, dostępny z poziomu BIOS lub szybkiego menu boot’owania.  System umożliwiający przetestowanie komponentów bez konieczności uruchamiania systemu operacyjnego. System musi posiadać wszystkie swoje funkcjonalności w przypadku: braku dysku, uszkodzenia dysku, sformatowania dysku, braku dostępu do sieci, internetu. Nie dopuszcza się stosowania wewnętrznych i zewnętrznych urządzeń w celu uzyskania funkcjonalności. Pełna obsługa systemu diagnostycznego za pomocą klawiatury i myszy jak i samej myszy. |
| Bezpieczeństwo | Dedykowany układ sprzętowy TPM min. 2.0 zgodny z certyfikacją TCG, przechowujący klucze kryptograficzne i certyfikaty.  Wbudowany czujnik otwarcia dolnej pokrywy obudowy.  Wbudowana w obudowę matrycy kamera IR umożliwiająca autentykację na poziomie oferowanego systemu operacyjnego  Wbudowany czytnik linii papilarnych  Wbudowany czytnik SmartCard |
| Zarządzanie zdalne | Wbudowana w płytę główną technologia zdalnego monitorowania i zarządzania komputerem na poziomie sprzętowym (out-of-band) działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC. Wymagana jest obsługa funkcji zdalnego zarządzania przez wbudowane w komputer porty zarówno sieci przewodowej LAN, jak i bezprzewodowej WLAN, z wykorzystaniem protokołów TCP/IP w tym IPv6 wraz z szyfracją komunikacji zarządzania z silnym protokołem minimum TLS 1.2 i zestawami silnych szyfrów TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384;TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 & TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 lub silniejszymi/nowocześniejszymi.  Technologia ta powinna być zgodna z otwartymi standardami DMTF WS-MAN 1.0.0 (<http://www.dmtf.org/standards/wsman> ) oraz DASH 1.2.0 (<http://www.dmtf.org/standards/mgmt/dash>) oraz  musi obsługiwać łącznie wszystkie następujące funkcje:   1. Zdalny odczyt konfiguracji komponentów komputera – model komputera i jego nr seryjny, model procesora, ilość, rodzaj i nr seryjne modułów pamięci RAM, model i nr seryjny dysku HDD/SSD, wersja BIOS FW płyty głównej, nr seryjny płyty głównej, dla laptopów model, znamionowa pojemność, numer seryjny i data produkcji baterii; 2. kontrolę stanu zasilania komputera pozwalającą na sprawdzenie aktualnego stanu zasilania komputera (stany ACPI S0/S3/S4/S5) oraz zdalne włączenie komputera ze stanu pełnego wyłączenia, hibernacji, uśpienia i tzw. Modern Standby (Connected Standby) oraz zdalne wyłączenie/reset bez udziału systemu operacyjnego; 3. zdalną konfigurację ustawień komputera przez interfejs BIOS setup w trybie graficznym lub tekstowym (ASCII). 4. zdalne przejęcie konsoli tekstowej systemu – tzw. Text Console Redirection lub Serial over LAN z możliwością jej wykorzystania do zdalnej zmiany ustawień BIOS Setup oraz odblokowania MS BitLocker Recovery. 5. zdalne przejęcie pełnej konsoli graficznej systemu tzw. KVM Redirection (Keyboard, Video, Mouse) na poziomie sprzętowym bez udziału systemu operacyjnego ani dodatkowych programów, również w przypadku braku lub uszkodzenia systemu operacyjnego do rozdzielczości 2560×1600 (WQXGA) włącznie zgodnie z profilem DSP1076 standardu DASH <https://www.dmtf.org/sites/default/files/standards/documents/DSP1076_1.0.1.pdf>   Funkcja przekierowania konsoli graficznej musi przechwytywać każdy rodzaj wyświetlanego na fizycznym lokalnym ekranie obrazu włącznie z procesem uruchamiania komputera (POST), odblokowania systemu szyfracji dysku, ładowania OS z dowolnego nośnika, zamykania OS oraz błędów ww. procesów: POST,ładowania OS (np. brak nośnika uruchamiającego, uszkodzenia OS BSOD (Blue Screen of Death) bez potrzeby modyfikacji tzw. loadera OS. |
| System operacyjny | Zainstalowany system operacyjny Windows 11 Pro, klucz licencyjny zapisany trwale w BIOS, umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego. |
| Oprogramowanie biurowe | Microsoft Office Home&Business 2024 PL |
| Oprogramowanie dodatkowe | Dołączone do oferowanego komputera oprogramowanie z nieograniczoną licencją czasowo na użytkowanie umożliwiające:  - upgrade i instalacje wszystkich sterowników, dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,  - możliwość przed instalacją sprawdzenia każdego sterownika, BIOS’u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji:                  a. o poprawkach i usprawnieniach dotyczących aktualizacji                  b. dacie wydania ostatniej aktualizacji                  c. priorytecie aktualizacji                  d. zgodność z systemami operacyjnymi                  e. jakiego komponentu sprzętu dotyczy aktualizacja  - wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne  - możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga.  - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr)  - sprawdzenia historii upgrade’u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania)  - dokładny wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu \*.xml  - raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach, zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku \*.xml. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.  Oprogramowanie umożliwiające aktualizację BIOS bezpośrednio z serwera producenta komputera przy wykorzystaniu bezpiecznego, szyfrowanego połączenia bez konieczności uruchamiania systemu operacyjnego oraz wykorzystywania zewnętrznych nośników pamięci masowej.  Oprogramowanie musi automatycznie rozpoznawać model urządzenia i bieżącą wersję BIOS. Oprogramowanie posiadające bezterminową licencję.  Możliwość zabezpieczenia dostępu do oprogramowania hasłem administratora.  Oprogramowanie umożliwiające przywrócenie obrazu systemu operacyjnego bezpośrednio z serwera producenta komputera przy wykorzystaniu bezpiecznego, szyfrowanego połączenia bez konieczności uruchamiania systemu operacyjnego.  W przypadku wystąpienia awarii oprogramowanie automatycznie uruchomi się i zapewni możliwość naprawy systemu operacyjnego lub przywrócenie go do stanu fabrycznego z możliwością dokonania kopii zapasowej plików przed uruchomieniem procesu.  Dodatkową funkcją oprogramowania jest możliwość wykonania kopii dysku (tzw. klonowania) wraz z plikami, ustawieniami aplikacji, systemem operacyjnym i jego ustawieniami.  Licencja pozwalająca na bezpłatne korzystanie z oprogramowania przez cały okres gwarancji komputera. |
| Porty i złącza | Wbudowane porty i złącza: 1 x HDMI 2.1, 2 x USB 3.2 typ A, 2 x Thunderbolt 4, RJ – 45, port audio combo, gniazdo linki zabezpieczającej  Nie dopuszcza się stosowania adapterów w celu osiągnięcia powyższych portów. |
| Warunki gwarancyjne, wsparcie techniczne | Min. 24 miesięczna 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.  W przypadku awarii dysk twardy zostaje u Zamawiającego.  Zamawiający wymaga narzędzia do zarządzania zgłoszeniami serwisowymi samodzielnie przez portal internetowy lub inne narzędzie nie wymagające działań po stronie dostawcy. Narzędzie powinno umożliwiać:  - samodzielne wystawianie zgłoszeń serwisowych, śledzenie stanu zgłoszenia, komunikację z serwisem producenta przez edycję zlecenia i stanu zlecenia  - dostęp do materiałów serwisowych - co najmniej podręczników serwisowych i not serwisowych  - dostęp do materiałów szkoleniowych  - możliwości dodawania plików do otwieranego lub otwartego zlecenia (zdjęcia uszkodzeń, opisy etc.)  - śledzenie historii zleceń - raporty ze zleceń, historia - dla poszczególnych zleceń lub dla poszczególnych komputerów  - możliwość rejestrowania i zarządzania zdarzeniami serwisowymi - agregowania zdarzeń z oprogramowania zarządzającego dostarczonego przez producenta, możliwość konwertowania zdarzeń na zgłoszenia serwisowe do producenta - z poziomu narzędzia.  - możliwość spięcia systemu serwisowego producenta z systemem helpdesk zamawiającego (dostępność API co najmniej dla opcji wystawienie zlecenia, sprawdzenie stanu zlecenia, raport zleceń) |

**INDEKS 27**

**Projektor – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagania minimalne** |
| Technologia wyświetlania | DLP |
| Źródło światła | Laser |
| Jasność | 4300 |
| Rozdzielczość | 1920x1080 px |
| Współczynnik proporcji | 16:9 |
| Kontrast | 300000 |
| Żywotność lampy | Min. 30000 h |
| Złącza | 1 x USB-A power 1.5A, 1x 3.5mm minijack, 1x RJ45, 1x RS232, 2x HDMI2.0 |
| Wbudowany głośnik | TAK |
| Poziom hałasu | Max. 31dB (tryb normal) |
| Gwarancja | Min 24 miesiące gwarancji producenta |

**INDEKS 32**

**Urządzenie wielofunkcyjne A3 – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagania minimalne** |
| Wymagania ogólne | Urządzenie wielofunkcyjne kolor (drukarka, kopiarka, skaner) format A3 wyposażone w komplet pełnowartościowych tonerów CMYK oraz fabryczną podstawę na kółkach |
| Prędkość urządzenia A4 | Do 25/25 str./min (mono/kolor) |
| Prędkość urządzenia A3 | Do 15/15 str./min (mono/kolor) |
| Prędkość druku dwustronnego | Do 45/45 str./min (mono/kolor) |
| Czas uzyskania pierwszej strony | Do 5,2/6.9 sekundy (mono/kolor) |
| Czas nagrzewania | Około 11/11 sekund (mono/kolor) |
| Technologia obrazowania | Laser |
| Technologia tonera | Toner polimeryzowany HD |
| Rozmiar panelu / rozdzielczość | min. 10“ / 1024 x 600 |
| Pamięć systemowa | Minimum 8 GB |
| Systemowy dysk twardy | 256GB SSD |
| Procesor | Procesor: co najmniej 4 rdzeniowy o wydajności co najmniej 1,6 GHz |
| Interfejs | 10/100/1,000-Base-T Ethernet; USB 2.0; |
| Protokoły sieciowe | TCP/IP (IPv4 / IPv6); SMB; LPD; IPP; SNMP; HTTP(S);Bonjour |
| Automatyczny podajnik dokumentów | Do 100 oryginałów; A6-A3; 35-163 g/m² |
| Obsługiwane formaty papieru | A6–SRA3; rozmiary własne; papier banerowy max. 1,200 x 297 mm |
| Obsługiwane gramatury papieru | 52–300 g/m² |
| Pojemność wejściowa papieru | 1150 arkuszy |
| Pojemność kaset podstawowa | 1x 500; A6–A3; rozmiary własne; 52–256 g/m²  1x 500; A5–SRA3; rozmiary własne; 52–256 g/m² |
| Podajnik ręczny | 150 arkuszy; A6–SRA3; rozmiary własne; baner; 60–300 g/m² |
| Automatyczny druk dwustronny | A6-SRA3; 52–256 g/m² |
| Pojemność tac wyjścia | Do 250 arkuszy |
| Obciążalność (miesięczna) | Maksymalna 130,000 stron |
| Wydajność tonera | Czarny do 28,000 stron CMY do 28,000 stron |
| Wydajność zespołów obrazowania | Czarny do 170,000/1,000,000 stron (bęben/developer) CMY do 65,000/1,000,000 stron (bęben/developer) |
| Zużycie energii | 220-240 V / 50/60 Hz; Mniej niż 1.6kW |
| Specyfikacja drukarki |  |
| Rozdzielczość druku | 1,800 x 600 dpi; 1200 x 1200 dpi |
| Język opisu strony | PCL 6 (XL3.0); PCL Sc; PostScript 3 (CPSI 3016); XPS |
| Systemy operacyjne | Windows 10 (32/64); Windows 11;;Windows Server 2019; Windows Server 2022;macOS 10.14 lub późniejszy; Unix; Linux; |
| Czcionki drukarki | 80 PCL Latin; 137 PostScript 3 Emulation Latin |
| Specyfikacja kopiarki |  |
| Rozdzielczość kopiowania | 600 x 600 dpi |
| Gradacja | 256 gradacji |
| Wielokrotność kopiowania | 1-9,999 |
| Format | Max. SRA3 |
| Powiększenie | 25-400% krokowa co 0,1%; automatyczne skalowanie |
| Specyfikacja skanera |  |
| Prędkość skanowania | Do 100 obrazów/min. jednostronnie Do 200 obrazów/min. dwustronnie |
| Rozdzielczość skanowania | Do 600 x 600 dpi |
| Rodzaje skanowania | Skanowanie do: e-mail; 5MB (do folderu domowego); FTP; BOX; USB; WebDAV; DPWS; URL, TWAIN |
| Typy plików | JPEG; TIFF; PDF; kompaktowy PDF; szyfrowany PDF; XPS; kompaktowy XPS; PPTX; PDF/A 1a i 1b |
| Specyfikacja skrzynek użytkownika |  |
| Przechowywanie dokumentów | Do 3,000 dokumentów lub 10,000 stron |
| Typy skrzynek użytkownika | Publiczne; osobiste (z hasłem lub autoryzacją); grupowe (z autoryzacją) |
| Typy skrzynek systemowych | Wydruk bezpieczny; wydruk szyfrowanych plików PDF |
| Funkcje systemu |  |
| Konta dostępu | (nazwa użytkownika + e-mail + folder smb); definiowanie funkcji dostępu użytkownika; |
| Oprogramowanie | Sterowniki dla obsługiwanych systemów operacyjnych, oprogramowanie zarządzające. |
| Inne |  |
| Dokumentacja | Wykonawca dostarczy urządzenie wraz z pełną dokumentacją techniczną i instrukcją obsługi w języku polskim |
| Gwarancja | Min. 24 miesiące |
| Rok produkcji | Urządzenie musi być fabrycznie nowe, wolne od wad prawnych i technicznych. Nie starsze niż 2025 rok. |
| Dostawa | Dostawa obejmuje transport, wniesienie i uruchomienie urządzenia. |
| Ustawienie | Urządzenie zaprojektowane i dostarczane przez producenta drukarki do pracy korytarzowej, podłogowej, umożliwiające obsługę urządzenia na korytarzu w pozycji stojącej. |
| Panel użytkownika | Informacja wyświetlana w języku polskim  Panel wbudowany w Urządzenie umożliwiający realizację usług kopiowania, drukowania i skanowania,  Ekran kolorowy, dotykowy, |
| Funkcje | Funkcje: drukowanie, kopiowanie i skanowanie.  Korzystania z funkcji skanowania, mimo braku tonerów. |
| Drukowanie i skanowanie | Wydruk, kopiowanie dwustronne: automatyczne  Skaner: dwustronny, automatyczny, mono i kolor, obsługujący skanowanie baneru o wymiarach 29,7 x 100 cm |
| Podstawa pod urządzenie | Na kółkach, zapewnia miejsce do przechowywania papieru |

**INDEKS 30**

**Urządzenie wielofunkcyjne A4 – 2 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagania minimalne** |
| Wymagania ogólne | Urządzenie wielofunkcyjne kolor (drukarka, kopiarka, skaner) format A4 |
| Prędkość druku A4 | do 43 str./min. |
| Prędkość druku A4 w trybie  Autoduplex | do 36 str./min. |
| Czas oczekiwania na pierwszy wydruk A4 | do 5.0 sek. |
| Czas nagrzewania | 14 sek. |
| Technologia obrazowania | Laserowa |
| Rozmiar panelu/rozdzielczość | Min. 5” |
| Pamięć systemu | 1 GB |
| Dysk systemowy | 2 GB eMMC |
| Interfejs | 10/100/1,000-Base-T Ethernet; USB 2.0, Wi-Fi |
| Protokoły sieciowe | TCP/IP (IPv4 / IPv6); SMB 3.0; IPP; SNMP; HTTP(S); |
| Automatyczny podajnik dokumentów | Do 50 oryginałów; A6-A4; jednoprzebiegowy |
| Obsługiwane formaty papieru | A6-A4; rozmiary niestandardowe |
| Obsługiwana gramatura papieru | 60-199 g/m² |
| Pojemność wejściowa papieru | 650 arkuszy |
| Podajnik boczny/uniwersalny | 100 arkuszy; A6-A4; rozmiary niestandardowe; |
| Pojemność wyjściowa | Do 150 arkuszy |
| Żywotność tonera wraz z zespołem obrazowania | Do 20500 stron |
| Zużycie energii | 220-240 V / 50/60 Hz; Mniej niż 1.43 kW |
| Wymiary max (szer. x gł. x wys.) | 480 x 600 x 460 mm |
| Waga maksymalna | 20 kg |
| Specyfikacja drukarki |  |
| Rozdzielczość druku | 1200 x 1200 dpi |
| System operacyjny | Windows 10 (32/64); Windows 11; Windows Server 2022; macOS 10.14 i nowsze; Unix; Linux |
| Specyfikacja skanera |  |
| Prędkość skanowania | Do 20 obr./min. w trybie jednostronnym  Do 34 obr./min. dwustronnie |
| Rozdzielczość skanowania | Do 600 x 600 dpi |
| Tryby skanowania | Scan-to-eMail; Scan-to-SMB; Scan-to-FTP; Scan-to-USB; |
| Formaty plików | JPEG; TIFF; PDF; Kompaktowy PDF; Szyfrowany PDF; XPS; Kompaktowy XPS; PPTX |
| Specyfikacja Kopiarki |  |
| Rozdzielczość kopiowania | 600 x 600 dpi |
| Gradacja | 256 gradacji |
| Kopiowanie wielokrotne | 1-9999 |
| Format oryginału | Max. A4 |
| Powiększenie | 25-400% krok co 1%; automatyczne skalowanie |
| Funkcje Systemu |  |
| Bezpieczeństwo | Filtrowanie IP i blokowanie portów; Komunikacja sieciowa TLS/1.3; Obsługa IPsec; Obsługa IEEE 802.1x; Uwierzytelnianie użytkownika PIN; Szyfrowanie danych użytkownika. Druk bezpieczny |
| Oprogramowanie | Sterowniki dla obsługiwanych systemów operacyjnych, oprogramowanie zarządzające. |
| Inne |  |
| Gwarancja | Minimum 24 miesiące realizowana na miejscu. Wykonawca wykonuje przegląd gwarancyjny 2 razy w roku – czyszczenie, kalibracja. |
| Dokumentacja | Wykonawca dostarczy urządzenie wraz z pełną dokumentacją techniczną i instrukcją obsługi w języku polskim |
| Rok produkcji | Urządzenie musi być fabrycznie nowe, wolne od wad prawnych i technicznych.  Nie starsze niż 2025 rok. |
| Dostawa | Dostawa obejmuje transport do siedziby zamawiającego, wniesienie i uruchomienie urządzenia. |
| Tonery i akcesoria | Wykonawca dostarczy urządzenie wraz z pełnowartościowym tonerem oraz wszystkimi akcesoriami niezbędnymi do uruchomienia. |
| Drukowanie i skanowanie | Wydruk, kopiowanie dwustronne: automatyczne Skaner: dwustronny, automatyczny, jednoprzebiegowy, mono i kolor. |

**INDEKS G6**

**Zestaw do skanowania i drukowania – 1 kpl.**

* drukarka etykiet

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Metoda druku | Termiczna\termotransferowa |
| Język programowania drukarki | EPLII  ZPLII |
| Rozdzielczość druku | 300 dpi |
| Szerokość druku | do: 104 mm |
| Szybkość drukowania | do: 152 mm/sek |
| Czujniki nośników | tak |
| Kody kreskowe | tak |
| Czcionki i grafika | tak |
| Druk pionowy | tak |
| Druk w poprzek | tak |
| Rozwiązania komunikacyjne | USB  Ethernet |
| Rodzaj zasilania | sieciowe AC (100-240V) |
| Energy Star | tak |
| Aplikacja do projektowania etykiet | Tak |
| Gwarancja | Min. 24 miesiące |
| Etykiety termiczne 50x30 | 5 x 2000 szt. |

* skaner dokumentów

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Technologia skanowania | Szczelinowa, jednoprzebiegowy skaner dwustronny (duplex) |
| Typ skanera | Automatyczny z podajnikiem dokumentów ADF |
| Panel sterowania | Kolorowy min. 10,5 cm |
| Rozdzielczość optyczna | Min. 600 dpi x 600 dpi |
| Prędkość skanowania (300 dpi) | Jednostronnie min. 45 str/min.  Dwustronnie min. 90 str/min. |
| Automatyczny podajnik dokumentów | Min. 100 arkuszy |
| Format dokumentu | Max.215,9 mm x 6096 mm (tryb długiego dokumentu)  Min. 50,8 mm x 50,8 mm |
| Dzienna wydajność | Do 7000 stron |
| Łączność | USB 3.0, Ethernet LAN, Wi-Fi, Wi-Fi Direct |
| Niezawodność | Wykrywanie zacięć i podwójnego podania arkuszy |
| Uwierzytelnianie | LDAP, dane logowania lub przez PIN, możliwość obsługi kart identyfikacyjnych |
| Zarządzanie systemem | Możliwość zdalnego kontrolowania przez administratora, konfiguracji kont użytkowników i procesów skanowania |
| Kompatybilność mobilna | Skanowanie z urządzeń mobilnych (telefon, tablet) iOS, Android |
| Obsługiwane platformy | Windows, Mac OS, iOS, Android, Chromebook, Cirtrix |
| Sterowniki | TWAIN |
| Gwarancja | Min. 24 miesiące |

* skaner ręczny typu „imager”

|  |  |
| --- | --- |
| Technologia skanowania | Wielokierunkowa, odczyt niezależnie od ułożenia skanera względem kodu |
| Rodzaj odczytywanych kodów | Obsługa kodów 1D (liniowych)  oraz 2D (QR code, Data Matrix, Code 128, interleaved 2 of 5) |
| Zasięg skanowania SR | Od 1,23 cm do 36,8 cm zależnie od gęstości kodu |
| Zasilanie | Przez kabel USB z hosta |
| Odporność na upadki | Urządzenie musi wytrzymać wielokrotne upadki na beton z wysokości 1,5 metra |
| Sygnalizacja odczytu | Dźwiękowa z możliwością regulacji głośności oraz wizualna |
| Tryby pracy | Ręczny oraz automatyczny po umieszczeniu w podstawce |
| Konfiguracja | Możliwość prostego programowania za pomocą skanowania kodów konfiguracyjnych |
| Rodzaj zasilania | sieciowe AC (100-240V) |
| Dodatkowe funkcję | Auto-enter |
| Gwarancja | Min. 24 miesiące |

**INDEKS 28**

**Ekran projekcyjny – 1 szt.**

Specyfikacja:

1. Typ ekranu: Rozwijany elektrycznie
2. Format 16:9
3. Szerokość ekranu: min. 300 cm
4. Wysokość ekranu: min. 227.5 cm
5. Szerokość obrazu: min. 290 cm
6. Wysokość obrazu: min. 163 cm
7. Czarne ramki boczne: min. 5 cm
8. Czarny TOP: min. 59.5 cm
9. Kąt widzenia: min. 160° °
10. Powierzchnia projekcyjna ze współczynnikiem odbicia światła 1.0
11. Technologia Plug and Play
12. Wyświetlanie obrazu jakości HD ready, Full HD oraz 4K
13. Czarny dół: 5 cm
14. Długość obudowy: max 309.6 cm
15. Przekrój kasety: max 10,5 x 9,5 cm

Obsługa:

1. Sterowanie: ścienne oraz bezprzewodowe
2. Rodzaj silnika: Tubowy
3. Płaska powierzchnia dolna - możliwość zabudowy w suficie
4. Pozycja zasilania: z lewej strony

Parametry techniczne:

1. Waga (netto) – max. 19 kg
2. Materiał obudowy: stal

Gwarancja – 3 lata

**INDEKS 3D**

**Monitor wielkoformatowy– 1 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagania minimalne** |
| Przekątna ekranu | Min. 55” |
| Proporcje ekranu | 16:9 |
| Rozdzielczość | 3840-2160 4K UHD |
| Jasność | Min. 300 cd/m2 |
| Kontrast | Min. 5000:1 |
| Czas reakcji | Max. 6.5ms |
| Tryb pracy ciągłej | TAK 24/7 |
| Żywotność ekranu | Min. 50 000 godzin |
| Głośniki | Tak 2x15W |
| Wbudowany CPU | Min. 8 rdzeniowy 2.2GHz |
| RAM | Min. 4GB |
| Łączność | WIFI, Bluetooth 5.0 |
| Złącza | 2 x USB Typ A (w tym 1x USB3.0), 3 x HDMI in 2.1 z HDCP 2.2, 1 x Audio Line Out, 1 x LAN In (RJ45), 1 x RS232, 1 x AV In |
| Gwarancja | Min. 24 miesiące |

**INDEKS 31A**

**Telefon TYP 1: 7 szt.**

Wymagania minimalne:

* Caller ID\*2 pamięcią 50 wpisów
* Wyraźny podświetlany ekran LCD
* Wygodny (Klawisz nawigacyjny)
* Wykonanie premium (słuchawka bezodciskowa) Książka telefoniczna z 50 rekordami
* Pamięć redial (do 10)
* Dzwonki do wyboru
* Połączenia konferencyjne
* Interkom Słuchawka – Słuchawka)
* Dzielenie połączenia
* Budzik i zegar
* Odbieranie każdym klawiszem
* Akumulator Ni-MH
* Montaż na ścianie SMS są dostępne tylko dla GR,FX,HG oraz PD
* Gwarancja min 24 miesiące

**INDEKS 31**

**Telefon TYP 2: 1 szt.**

Wymagania minimalne

* Wyświetlacz: Kolorowy, dotykowy LCD 4.3 cala z 5 programowalnymi polami BLF-VIP (Busy Lamp Field).
* Przyciski: 19 fizycznych przycisków z BLF (programowalne, np. do szybkich połączeń, statusów).
* Złącza: 2x Jack 3.5mm (słuchawki nagłowne/mikrofon), gniazdo rozszerzeń (EXT) do konsol/komputera.
* Zasilanie: Z linii (analog) lub PoE (IP) lub opcjonalny zasilacz 12V.
* Łączność (wersja IP): Przyłączenie przez RJ45 do sieci Ethernet, wbudowany switch.
* Zarządzanie: Profile przechowywane w centrali, łatwa instalacja (Plug & Play).
* Dodatki: Obsługa słuchawek bezprzewodowych EHS (z adapterem)
* Gwarancja min. 24 miesiące

**INDEKS 3E**

**Centrala telefoniczna: 1 szt.**

Wymagania minimalne

* Obudowa: rack 1U do montażu w szafie RACK
* Rodzaje łącz: IP, GSM, ISDN, POTS
* Sloty rozbudowy: 4 wolne sloty na karty rozszerzeń
* Porty wewnętrzne AB: min. 14
* Linie miejskie POTS: min. 5
* Nagrywanie rozmów: 8 kanałów nagrywania na karcie microSD (do 8GB).
* Kanały IP: min. 8
* Ilość abonentów IP (SIP) – min. 24
* Parametry VOIP:
  + Obsługiwane protokoły: eSSL, SIP 2.0 kodek G.711a
  + Tryb pracy: klient lub / i serwer VoIP
* Funkcje: Identyfikacja abonenta (CLIP), przenoszenie/przekazywanie połączeń, zaawansowane zarządzanie kosztami, 99 zapowiedzi słownych (DISA/Infolinia), integracja CTI (TAPI, XML).
* Automatyka: 1 sensor / 1 przekaźnik do sterowania urządzeniami zewnętrznymi.
* Interfejs LAN: 1 port Ethernet 10/100 Mbps.
* Zasilanie: Standardowe zasilanie, możliwość zasilania awaryjnego z modułem akumulatorów.
* Wymiary: Obudowa 1U do montażu w szafie RACK (310x210x55 mm).
* Centrala rozbudowana o karty rozszerzeń:
  + dwa dodatkowe porty abonentów wewnętrznych (FXS)
  + jeden dodatkowy port abonenta systemowego (CTS)
* Funkcje dodatkowe: Współpraca z telefonami systemowymi Slican (Upo, IP, SIP). Integracja z oprogramowaniem Slican BillingMAN, PhoneCTI, MobileCTI. Obsługa domofonów Slican (jako abonent wewnętrzny).
* Dołączona licencja VoIP na 2 kanały

**INDEKS 33**

**Niszczarka biurowa: 3 szt.**

Wymagania minimalne

* Niszczarka do dokumentów przeznaczona do użytku w małych biurach lub do użytku indywidualnego.
* Obsługuje papier biurowy, zszywki, spinacze, karty plastikowe (np. karty kredytowe), płyty CD/DVD. Cięcie i poziom bezpieczeństwa
* Rodzaj cięcia: paski (strip-cut).
* Szerokość pasków: 5,8 mm
* Klasyfikacja bezpieczeństwa (według normy DIN 66399): E-2 / 0-2/ P-2 / T-2. wydajności i pojemności
* Jednorazowa ilość niszczonych kartek (papier 80 g/m²): 17-19 arkuszy.
* Szerokość szczeliny wlotowej: 230 mm (dla formatu A4).
* Pojemność kosza na ścinki: 25 litrów.
* Wymiary i waga Wymiary (szer. x głęb. x wys.): 365 x 280 x 542
* Waga urządzenia: 9,8 kg.
* Zasilanie i zużycie energii
* Napięcie: 220-240 V, częstotliwość: 50 Hz.
* Pobór mocy silnika: 360 W.
* Tryb czuwania (standby): bardzo niski pobór energii (system oszczędzania energii)