**Opis przedmiotu zamówienia**

**na systemy informatyczne- Załącznik nr 1 do SWZ**

Spis treści

[Zastrzeżenia: 3](#_Toc131771845)

[Część 1 – dostawa serwera bazodanowego do Banku Krwi wraz z migracją systemu 5](#_Toc131771846)

[Charakterystyka sprzętu (wymagania minimalne) 5](#_Toc131771847)

[Prace dodatkowe 7](#_Toc131771848)

[Wymagana dokumentacja 8](#_Toc131771849)

[Wymagana dotyczące realizacji zamówienia 8](#_Toc131771850)

[Część 2 – dostawa systemów serwerowych 9](#_Toc131771851)

[Serwery x86 – 2 szt. 9](#_Toc131771852)

[Wdrożenie usługi Active Directory 13](#_Toc131771853)

[Zasilacze awaryjne UPS – 9 szt. 15](#_Toc131771854)

[Oprogramowanie do wirtualizacji 16](#_Toc131771855)

[Część 3 – dostawa komputerów, laptopów, peryferii i akcesoriów, oprogramowania 19](#_Toc131771856)

[Zestaw komputerowy standardowy – 45 szt. 19](#_Toc131771857)

[komputer standardowy – 45 szt. 19](#_Toc131771858)

[monitor standardowy – 45 szt. 23](#_Toc131771859)

[Laptop – 35 szt. 23](#_Toc131771860)

[Zaawansowana stacja robocza – 4 szt. 24](#_Toc131771861)

[stacja robocza – 4 szt. 24](#_Toc131771862)

[monitor zawansowany – 8 szt. 27](#_Toc131771863)

[Drukarka igłowa – 1 szt. 28](#_Toc131771864)

[Tester sieciowy 10G z obsługą PoE 28](#_Toc131771865)

[Oprogramowanie biurowe – 55 licencji 29](#_Toc131771866)

[Część 4 – dostawa aktywnych urządzeń sieciowych 33](#_Toc131771867)

[Przełączniki systemowe 33](#_Toc131771868)

[Switch 48 port – 2 szt. 33](#_Toc131771869)

[Switch 48 port PoE – 3 szt. 35](#_Toc131771870)

[Switch 8x SFP+ 8x 10GbE – 1 szt. 36](#_Toc131771871)

[Switch 12x SFP+ 12x 10GbE – 1 szt. 38](#_Toc131771872)

[Przełączniki zdalne 40](#_Toc131771873)

[Switch 8p 1xPoE-PD – 15 szt. 40](#_Toc131771874)

[Switch 5p PoE – 4 szt. 41](#_Toc131771875)

[Switch 16p – 3 szt. 42](#_Toc131771876)

[Część 5 – Oprogramowanie monitorujące sieć 45](#_Toc131771877)

[Część 6 – dostawa macierzy dyskowych sieciowych (NAS) – 2 szt. 53](#_Toc131771878)

[NAS 1: 53](#_Toc131771879)

[NAS 2: 53](#_Toc131771880)

[Specyfikacja wspólna dla NAS: 53](#_Toc131771881)

[Wymagania ogólne: 53](#_Toc131771882)

[Wdrożenie 54](#_Toc131771883)

[Część 7 – dostawa i wdrożenie firewalla NG UTM – 2 szt. w klastrze 55](#_Toc131771884)

[Wymagania Ogólne 55](#_Toc131771885)

[System logowania i raportowania 60](#_Toc131771886)

[Wymagania dotyczące wdrożenia 62](#_Toc131771887)

[Część 8 – dostawa oprogramowania do backupu 65](#_Toc131771888)

# Zastrzeżenia:

1. W przypadku, gdy opis przedmiotu zamówienia został opisany przez wskazanie znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę Zamawiający dopuszcza rozwiązania równoważne opisywanym, a wskazaniu takiemu towarzyszą wyrazy „lub równoważny”: Wszelkie nazwy własne znajdujące się w OPZ – np. dotyczące urządzeń będących komponentami zestawu komputerowego, oprogramowania, nie mogą być w żaden sposób traktowane jako rekomendacja ich nabycia, użycia, czy promocji.
2. Powołanie nazwy własnej w OPZ nie może być interpretowane jako ocena właściwości danego urządzenia czy programu komputerowego, ani tym bardziej jako przesłanka uznania ich za lepsze od innych analogicznych urządzeń czy innego porównywalnego oprogramowania.
3. Urządzenia muszą być dostarczone w stanie fabrycznie nowym, wolnym od wad technicznych, prawnych i formalnych zwłaszcza w zakresie licencji i uprawnień do aktualizacji oprogramowania. Sprzęt nie może być wcześniej zarejestrowany na żadnego innego klienta w bazie klientów producenta sprzętu.
4. Zamawiający może przed podpisaniem protokołu odbioru sprzętu zażądać oświadczenia producenta na podstawie numerów seryjnych, że oferowany sprzęt jest nowy i pochodzi z legalnego kanału dystrybucyjnego producenta. Jeśli sprzęt nie spełnia tych warunków Zamawiający odstąpi od umowy z winy Oferenta.
5. Serwis urządzeń musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta.
6. Dostarczone licencje powinny pochodzić z oficjalnego kanału dystrybucyjnego producenta na rynek polski. Licencje muszą być aktywowane po raz pierwszy, nie dopuszcza się licencji przenoszonych od innych użytkowników.
7. Pozycje opisane jako *Wyposażenie dodatkowe* oznaczają elementy lub akcesoria, które nie muszą pochodzić od producenta pozycji głównej, jeśli nie określono inaczej gwarancja na te pozycje wynosi 12 miesięcy. Wyposażenie dodatkowe należy uwzględnić w cenie pozycji głównej.
8. Gwarancja na dyski twarde (HDD, SSD, NVMe) w każdym przypadku obejmuje opcję zachowania przez Zamawiającego wadliwego dysku w przypadku jego awarii.

Strona celowo pozostawiona pusta.

# Część 1 – dostawa serwera bazodanowego do Banku Krwi wraz z migracją systemu

Dostawa, instalacja, nadzór i serwis serwera bazodanowego na potrzeby Regionalnego Centrum Krwiodawstwa i Krwiolecznictwa w Lublinie.

|  |  |  |
| --- | --- | --- |
| **1** | Charakterystyka sprzętu (wymagania minimalne) | **Ilość** |
| 1.1 | 4-core Typical 2.3 to 3.8 Ghz (max) POWER9 Processor | 1 |
| 1.2 | Mirrored System Disk Level, Specify Code | 1 |
| 1.3 | IBM i Operating System Partition Specify | 1 |
| 1.4 | Primary OS - IBM i | 1 |
| 1.5 | Factory Deconfiguration of 1-core | 3 |
| 1.6 | Rack Indicator- Not Factory Integrated | 1 |
| 1.7 | Software Preload Required | 1 |
| 1.8 | PowerVM Enterprise Edition | 1 |
| 1.9 | Sys Console On HMC | 1 |
| 1.10 | PCIe2 4-port 1GbE Adapter | 1 |
| 1.11 | Power Cord 4.3m (14-ft), Drawer to IBM PDU (250V/10A) | 2 |
| 1.12 | New IBM i License Core Counter | 1 |
| 1.13 | Other IBM i License Core Counter | 3 |
| 1.14 | Language Group Specify - Polish | 1 |
| 1.15 | SP Warranty Service Upgrade 3Y 24x7 CFix 24h | 1 |
| 1.16 | SP HDR/MR POWER 3Y | 1 |
| 1.17 | AC Power Supply - 1400W for Server (200-240 VAC) | 2 |
| 1.18 | IBM i 7.4 Indicator | 1 |
| 1.19 | SAS AE1 Cable 4m - HD Narrow 6Gb Adapter to Enclosure | 1 |
| 1.20 | System Port Converter Cable for UPS | 1 |
| 1.21 | PCIe3 SAS Tape/DVD Adapter Quad-port 6Gb x8 | 1 |
| 1.22 | Storage Backplane Gen4 with 2 NVMe U.2 drive slots | 1 |
| 1.23 | Rack-mount Rail Kit | 1 |
| 1.24 | Front IBM Bezel for 6 SAS + 4 NVMe -Bays BackPlane | 1 |
| 1.25 | #ES1H Load Source Specify (3.2 TB 4K NVMe U.2 SSD for IBM i) | 1 |
| 1.26 | 16 GB DDR4 Memory | 4 |
| 1.27 | 400 GB IBM i NVMe Load Source Namespace size | 1 |
| 1.28 | 4-core Typical 2.3 to 3.8 Ghz (max) POWER9 Processor | 1 |
| 1.29 | One Processor Core Activation for #EP50 | 4 |
| 1.30 | Enterprise 3.2 TB SSD PCIe4 NVMe U.2 module for IBM i | 2 |
| 1.31 | S&H-b | 1 |
| 1.32 | 1TB Removable Disk Drive Cartridge | 1 |
| 1.33 | Operator Panel LCD Display | 1 |
| 1.34 | Cable Ties & Labels | 1 |
| 1.35 | Express Edition 4 core (IBM i) | 1 |
| 1.36 | 2TB Removable Disk Drive Cartridge (RDX) | 1 |
| 1.37 | RDX USB External Docking Station | 1 |
| 1.38 | Standalone USB DVD drive w/cable | 1 |
| 1.39 | Multi-media Enclosure | 1 |
| 1.40 | Ultrium Cleaning Cartridge | 1 |
| 1.41 | HHLTO7 SAS Tape Drive | 1 |
| 1.42 | Attached to i5 OS & OS/400 System | 1 |
| 1.43 | Rack Device to PDU Cord | 1 |
| 1.44 | 5.5m Mini-SAS/Mini-SAS 1x Cable | 1 |
| 1.45 | Shipping and Handling - Charge | 1 |
| 1.46 | SP WAMO 3Y 24x7 CF24h | 1 |
| 1.47 | System i HIPO | 1 |
| 1.48 | Model 9009-41G Routing | 1 |
| 1.49 | IBM i (57xx-SS1) | 1 |
| 1.50 | Query (57xx-QU1) | 1 |
| 1.51 | DB2 Query (57xx-ST1) | 1 |
| 1.52 | Client Access - Processor Based (57xx-XW1) | 1 |
| 1.53 | English Primary Language U/L SBCS | 1 |
| 1.54 | Version 7 Release 4 | 1 |
| 1.55 | Preload | 1 |
| 1.56 | IBM i New or Transferred Licenses | 1 |
| 1.57 | IBM i Unlimited Users Mfg Key | 1 |
| 1.58 | Polish SBCS Secondary Language | 1 |
| 1.59 | Rack Not Integrated in Mfg Specify | 1 |
| 1.60 | 9009-41G ServicePac Warranty Service Upgrade 2 YR 24x7 Committed Fix 24h | 1 |
| 1.61 | 7226-1U3 ServicePac Warranty and Maintenance Option 2 YR 24x7 Committed Fix 24h | 1 |
| 1.62 | 9009-41G ServicePac for Hard Drive Retention for Power 2 years | 1 |
| 1.64 | 3-Year Registration SWMA for 5765-HMV/HMW/VHX | 1 |
| 1.65 | Per Install SW Maint 3Y Reg | 1 |
| 1.66 | System Software | 1 |
| 1.67 | DVD Process Charge | 1 |
| 1.68 | NovaLink (5765-PVS/PVE/VE3) | 1 |
| 1.69 | IBM PowerVM V3 VIOS | 1 |
| 1.70 | IBM PowerVM V3 Expansion Pack | 1 |
| 1.71 | DVD/CD-ROM | 1 |
| 1.72 | IBM SW Maintenance for IBM i and Selected Products, 3-Year Extended Registration | 1 |
| 1.73 | SWMA Renewal Registration | 1 |
| 1.74 | P05 Per Processor 3-Year Extended | 1 |
| 1.75 | IBM PowerVM Enterprise Edition V3 | 1 |
| 1.76 | Per Processor Core N/C (Small) | 1 |
| 1.77 | Hardware Management Console Virtual Appliance x86 based V10 | 1 |
| 1.78 | Electronic SW Delivery (ESD) | 1 |
| 1.79 | HMC Virtual Appliance V10 | 1 |
| 1.80 | Per Install | 1 |
| 1.81 | National Languages and Backup Media for IBM i V7 | 1 |
| 1.82 | i 7.4 Licensed Machine Code - RS 740-K (TR7) (2022-December-02) | 1 |
| 1.83 | Polish Secondary Language (i7.4) | 1 |
| 1.84 | ePoE Registration - Secondary Language | 1 |
| 1.85 | IBM Query for i | 1 |
| 1.86 | Preload Specifier | 1 |
| 1.87 | Supply Lang Group 2 (i7.4) | 1 |
| 1.88 | P05 OTC | 1 |
| 1.89 | IBM i V7 | 1 |
| 1.90 | Preload Specifier | 1 |
| 1.91 | Supply IBM i Lang Group 2 (i7.4) | 1 |
| 1.92 | i 7.4 Licensed Machine Code - RS 740-K (TR7) (2022-December-02) | 1 |
| 1.93 | i 7.4 USB Licensed Machine Code-RS 740-K (TR7) (2022-December-02) | 1 |
| 1.94 | IBM i per Core Registration | 1 |
| 1.95 | ePoE Registration | 1 |
| 1.96 | IBM i Access Client Solutions (XJ1) | 1 |
| 1.97 | IBM i Unlimited Users Registration | 1 |
| 1.98 | IBM i per Core (E4x/41x/22x/21A/VSN) | 1 |
| 1.99 | IBM i V7 | 1 |
| 1.100 | OTC Keyed SW Media | 1 |
| 1.101 | IBM i per Processor License Billing | 1 |
| 1.102 | OTC per Core w/ 90-Day SWMA (E4x/41x/21A/22G/VSN P05 Tier) | 1 |
| 1.103 | IBM i per User Billing | 1 |
| 1.104 | BOTC Unlimited Users (E4x/41x/21A/22G/VSN P05 Tier) | 1 |
| 1.105 | IBM DB2 Query Manager and SQL Development Kit for i | 1 |
| 1.106 | Preload Specifier | 1 |
| 1.107 | Supply Lang Group 2 (i7.4) | 1 |
| 1.108 | P05 OTC | 1 |
| 1.109 | IBM i Access Family | 1 |
| 1.110 | Preload Specifier | 1 |
| 1.111 | Supply PB Lang Group 2 (i7.4) | 1 |
| 1.112 | P05 OTC Charged with HW | 1 |
| 1.113 | Taśmy do dedykowanego napędu PCIe3 SAS Tape | 12 |
| 1.114 | 24 miesięczna gwarancja w wariancie 7/24 z opcją pozostawienia dysków w razie konieczności ich wymiany |  |

|  |  |
| --- | --- |
| **2** | Prace dodatkowe |
| 2.1 | Przeniesienie danych z dotychczasowego serwera na nowy serwer |
| 2.2 | Konfiguracja sieci LAN w taki sposób, aby stacje robocze pracowały z nowym serwerem |
| 2.3 | Podłączenie i konfiguracja (uruchomienie produkcyjne) aplikacji BANK KRWI wraz z systemem wspomagającym zarządzanie autorstwa ASSECO S.A. na nowym serwerze |
| 2.4 | Konfiguracja i weryfikacja transmisji danych z aparatów diagnostycznych na nowym serwerze |
| 2.5 | Konfiguracji i weryfikacji podłączonych drukarek do nowego serwera w szczególności drukarek do etykiet |
| 2.6 | Migracja licencji MIMIX + iOptomize wraz z upgrade do najnowszej wersji, migracja, instalacja, testy, szkolenie. |
| 2.7 | Podniesienie systemu operacyjnego na aktualnym serwerze produkcyjnym do wersji zgodnej z zamawianym serwerem i utrzymanie gwarancji oprogramowania na 1 rok |
| 2.8 | Konfiguracja KRDK na nowym serwerze |
| 2.9 | Konfiguracja systemu raportującego Cognos |
| 2.10 | Integracja nowego serwera z oprogramowaniem e- hemofilia |
| 2.11 | Konfiguracja prawności działania oprogramowania do ekstrakcji danych do systemu e-Krew na nowo dostarczonym serwerze |
| 2.12 | Szkolenie z zakresu obsługi nowego serwera. |

|  |  |
| --- | --- |
| **3** | Wymagana dokumentacja |
| 3.1 | Instrukcja użytkowania dostarczonego sprzętu i oprogramowania w języku polskim dopuszczalna wersja elektroniczna |
| 3.2 | Dokumentacja przeprowadzonej kwalifikacji/walidacji serwera. |
| 3.3 | Karta gwarancyjna, na całe urządzenie. |

|  |  |
| --- | --- |
| **4** | Wymagana dotyczące realizacji zamówienia |
| 4.1 | Termin realizacji zamówienie – do 180 dni od dnia podpisania umowy. |
| 4.2 | Dostawa, instalacja, uruchomienie przedmiotu zamówienia w miejscu użytkowania wskazanym przez Kupującego. |
| 4.3 | Transport krajowy i zagraniczny wraz z ubezpieczeniem, wszelkie opłaty celne, skarbowe oraz inne opłaty pośrednie - po stronie Oferenta. |
| 4.4 | O terminie dostawy przedmiotu zamówienia Oferent zawiadomi Kupującego z siedmiodniowym wyprzedzeniem. |
| 4.5 | Potwierdzeniem przez Kupującego: |
| 1. dostarczenia, odbioru, montażu, instalacji i bezawaryjnego rozruchu całości przedmiotu zamówienia, |
| 2. wraz z realizowaniem wymaganych szkoleń przez Oferenta będzie „Protokół odbioru” podpisany przez strony, który będzie stanowił podstawę do wystawienia faktury VAT. |
| 4.6 | Dostawa, instalacja, uruchomienie przedmiotu zamówienia w miejscu użytkowania wskazanym przez Kupującego w tym: |
| 1. dostarczenie sprzętu wraz z wniesieniem do miejsca przeznaczenia, |
| 2. instalacja i uruchomienie sprzętu, |
| 3. przeprowadzenie procedury kwalifikacji i walidacji zgodnie z IQ/OQ w miejscu instalacji, - po stronie Oferenta |

# Część 2 – dostawa systemów serwerowych

Zamówienie obejmuje dostawę 2 serwerów z systemami operacyjnymi, licencjami dostępowymi dla 250 użytkowników, wdrożenie usługi Active Directory, dostawę licencji i wdrożenie systemu wirtualizacji, 9 zasilaczy awaryjnych UPS.

Przed przystąpieniem do realizacji zadania Wykonawca ustali z Zamawiającym harmonogram realizacji prac. W dni szkoleń nie należy planować innych prac.

## Serwery x86 – 2 szt.

|  |  |
| --- | --- |
| Nazwa komponentu | Wymagane minimalne parametry techniczne |
| Obudowa | Obudowa Rack o wysokości maksymalnie 2U z możliwością instalacji min. 8 dysków SAS/SATA 2,5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. Obudowa musi posiadać ramkę zabezpieczającą zamykaną na klucz z przodu serwera w celu zabezpieczenia dysków przed wyjęciem. |
| Płyta główna | Płyta główna z możliwością zainstalowania do dwóch procesorów. |
| Chipset | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. |
| Procesor | Zainstalowane dwa procesory (każdy procesor posiadający maksymalnie 8 rdzeni), o prędkości bazowej min. 3,2 Ghz, w pełni obsługujące pamięci DDR4 RDIMM 2933Mhz. Wynik wydajności procesorów zainstalowanych w oferowanym modelu serwera, w systemie dwuprocesorowym, powinien wynosić min. 172 w teście SPECrate®2017\_fp\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. |
| Pamięć RAM | Minimum 256 GB RAM DDR4 RDIMM 3200MT/s, w modułach po 32 GB RAM.  Na płycie głównej powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci RAM |
| Zabezpieczenie pamięci | ECC, Memory Mirroring, SDDC, Memory Self-Healing lub PPR, Failed DIMM Isolation, Memory Thermal Throttling, Adaptive Double Device Data Correction (ADDDC), Memory Rank Sparing |
| Pamięć masowa | Zainstalowane dysków serwerowych SSD SATA o pojemności min. TB, 2,5“ Hot-Plug każdy.  Zainstalowany sprzętowy kontroler RAID umożliwiający skonfigurowanie RAID: 0, 1, 5, 6, 10, 50, posiadający 4GB pamięci cache oraz podtrzymanie pamięci na wypadek awarii zasilania lub pamięć nieulotną 4GB NV.  Zainstalowane dwa dyski M.2 SATA, każdy o pojemności min. 240GB Hot-Plug z możliwością konfiguracji RAID 1 za pomocą dedykowanego kontrolera RAID. Dyski wyposażone w diodę informującą o statusie pracy dysku .Rozwiązanie umożliwiające instalację dysków M.2 nie może powodować zmniejszenia ilości wnęk na dyski twarde. |
| Wbudowane porty | 4 x USB z czego nie mniej niż 2x USB 3.0 oraz USB TYP-C na przednim panelu obudowy i  2xVGA z czego jeden na panelu przednim. Złącze USB TYP-C na przednim panelu musi umożliwiać dostęp do karty zarządzającej serwera przez komputer PC z systemem Windows lub urządzenia mobilne z systemem Android. |
| Interfejsy sieciowe | Zainstalowane i w pełni funkcjonalne interfejsy:  - minimum 1 x RJ-45 Ethernet management port,  - minimum 2 karty sieciowe standardzie OCP umożliwiające wymianę w trybie hot-swap:  -pierwsza karta wyposażona w 2 porty 10Gb Ethernet w standardzie Base-T RJ45;  -druga karta wyposażona w 2 porty 1Gb Base-T RJ45; |
| Karta graficzna | Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200, dedykowana pamięć układu graficznego min. 32MB |
| Wentylatory | Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1 |
| Zasilanie | Minimum dwa identyczne zasilacze zainstalowane wewnątrz serwera, pracujące redundantnie, zapewniające możliwość wyłączenia i wyjęcia dowolnego z nich z serwera bez przerywania pracy serwera oraz bez ograniczania wydajności serwera, o mocy każdego zasilacza minimum 700W i sprawności na poziomie Titanium potwierdzoną certyfikatem 80 PLUS COMPLIANT dostępnym na stronie <https://www.clearesult.com/80plus/> |
| Bezpieczeństwo | Wbudowany czujnik otwarcia obudowy jako fabryczne rozwiązanie producenta. |
| Diagnostyka | Serwer wyposażony w wyświetlacz LED lub LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie serwera i kodach błędów. |
| Zarządzanie | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej; * zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); * szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; * możliwość podmontowania zdalnych wirtualnych napędów; * wirtualną konsolę z dostępem do myszy, klawiatury; * wsparcie dla IPv6; * wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; * możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; * integracja z Active Directory; * możliwość obsługi przez dwóch administratorów jednocześnie; * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. * możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera * Power-on password   Wykonawca w ramach oferty dostarczy oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające zdalne zarządzanie wszystkimi dostarczonymi serwerami jako grupą serwerów (klastrem), posiadające interfejs graficzny dostępny z poziomu przeglądarek internetowych (HTML), pozwalające na:   * włączenie, wyłączenie, restart, podgląd logów serwerów, sprawdzenie statusu sprzętu, przejęcie pełnej konsoli graficznej i tekstowej serwerów, * tworzenie szablonów instalacyjnych dla systemów operacyjnych, * tworzenie profili serwerów ze zdefiniowanymi parametrami BIOS, procesora/-ów, pamięci, kontrolera RAID które umożliwiają szybkie wdrożenie identycznej konfiguracji na grupie serwerów. * zdalne montowanie obrazów ISO pozwalające na uruchomienie z nich serwera, aktualizacja sterowników i BIOS serwerów zgodnie z stworzonym harmonogramem * monitorowanie stanu serwerów innych producentów za pomocą SNMP oraz umożliwiać przekierowanie bezpośrednio do karty zarządzającej wskazanego serwera * zbieranie statystyk zużycia energii, procesora/-ów, pamięci i temperatury dla wszystkich serwerów z możliwością graficznej prezentacji danych historycznych w formie wykresów do 5 lat wstecz. * Tworzenie mapy zainstalowanych urządzeń z podziałem na lokalizacje i szafy rack z graficzną prezentacją zajętości każdej z szaf rack * Logowanie w trybie SSO do karty zarządzającej posiadanych serwerów. * Oprogramowanie musi posiadać możliwość monitorowania za pomocą protokołów Redfish, SNMP serwerów innych producentów.   Oprogramowanie musi posiadać licencję na podłączenie co najmniej dostarczanych serwerów oraz wsparcie producenta na okres równy oferowanej gwarancji serwerów.  Serwer musi posiadać możliwość zarządzania z poziomu darmowej aplikacji mobilnej producenta serwera na urządzenia z systemami iOS oraz Android. Aplikacja musi umożliwiać podłączenie do serwera przez sieć IP lub przez port USB na froncie obudowy. Aplikacja musi umożliwiać:   * sprawdzenie aktualnego poboru mocy przez zasilacze * sprawdzenie temperatury powietrza na wlocie do serwera * sprawdzenie modelu kontrolera RAID oraz utworzonych dysków fizycznych i logicznych * sprawdzenie ilości zainstalowanych modułów pamięci, pojemności, taktowania, numerów seryjnych i slotu w którym są zainstalowane * sprawdzenie zainstalowanych procesorów , taktowania zegara ilości rdzeni, wątków oraz pamięci Cache * wyświetlanie alarmów dot. pracy serwera z podziałem na kategorie według istotności * konfiguracje adresacji IP portu management port * zmianę nośnika z którego serwer ma się bootować * wybór trybu pracy BIOS * włączenie oraz wyłączenie serwera * sprawdzenie wersji firmware * pobranie logów serwera |
| Certyfikaty | Serwer musi być wyprodukowany zgodnie z normą ISO 9001 oraz ISO 14001 lub równoważnymi.  Serwer musi być serwisowany zgodnie z normą ISO 9001 lub równoważną.  Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022 oraz Vmware w wersji min. 7.0. |
| Gwarancja | Wymagany jest serwis gwarancyjny 24 miesiące świadczony w trybie 9x5 OnSite przez 5 dni w tygodniu z gwarantowanym czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia.  Zamawiający wymaga, aby usługi serwisowe świadczone były wyłącznie przez producenta oferowanego sprzętu lub przez jego autoryzowany serwis.  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.  W przypadku awarii dysku twardego uszkodzony dysk pozostaje u Zamawiającego. |
|  |  |
| Wyposażenie dodatkowe | Przewód zasilający IEC C14 - IEC C13 3 m – 1 szt.,  Przewód zasilający wtyk uniwersalny (DIN49441) - IEC C13 3 m – 1 szt.,  Patchcord S/FTP kat.6A PiMF 2x RJ45 linka 5m – 4 szt.,  Wyposażenie dodatkowe nie musi pochodzić od producenta serwera, gwarancja 12 mies., należy uwzględnić w cenie serwera. |
| System operacyjny | Licencje Windows Server 2022 z prawem uruchomienia 4 instancji systemu, wersja polska, licencja CSP w modelu dożywotnim lub równoważny system serwerowy. Dostarczone licencje powinny pochodzić z oficjalnego kanału dystrybucyjnego producenta na rynek polski.  Równoważne oprogramowanie serwerowe musi umożliwić uruchomienie oprogramowania dziedzinowego użytkowanego aktualnie przez zamawiającego (systemy R2 Płatnik, Symfonia ERP, LIS Nautilus LAB) oraz pełną współpracę z ActiveDirectory,. Dostarczone licencje powinny pochodzić z oficjalnego kanału dystrybucyjnego producenta na rynek polski.  - Licencja bez ograniczeń czasowych. Warunki licencjonowania muszą zezwalać na zmianę wersji systemu operacyjnego na niższą z zachowaniem wsparcia technicznego oraz na przeniesienie licencji systemu operacyjnego na inny fizyczny serwer.  - instalacja i użytkowanie aplikacji 32- i 64-bitowych na dostarczonym serwerowym systemie operacyjnym;  - obsługa 2 procesorów fizycznych oraz co najmniej 16 core  - w ramach licencji zawarte prawo do wirtualizacji czterech systemów (OSE) na zasobach sprzętowych serwera; |

## Wdrożenie usługi Active Directory

Implementacja usługi katalogowej systemu Windows Server obejmująca co najmniej:

Dostawa licencji CAL per user 250 szt. W wersji zgodnej z systemami operacyjnymi dostarczanych serwerów,

Analiza przedwdrożeniowa

Projekt techniczny zawierający opis uzgodnionych i zaplanowanych prac, nazewnictwa elementów, struktury lasu, struktury domeny.

Wdrożenie AD na 2DC na VM

Utworzenie domeny,

Utworzenie schematu organizacyjnego

Wdrożenie WSUS (+ konfiguracja 10 PC pilotażowych)

Integracja NAS z AD QNAP lub Synology

Wdrożenie serwera wydruku 10 drukarek

Konfiguracja AD (GPO, LAPS, RODO, BitLocker)

Konfiguracja usługi rozpoznawania nazw domenowych DNS oraz nazw NetBIOS

Konfiguracja usługi przydzielania adresów oraz konfiguracji opcji TCP/IP

Konfiguracja polityki zabezpieczeń na podstawie dobrych praktyk branżowych, wgranie przykładowych polis, konfiguracja rekomendowanych zabezpieczeń dla środowiska stacji roboczych oraz systemów serwerowych.

Pilot migracji komputerów do domeny + procedura dalszej migracji – pilot na 10 PC

Warsztat dla administratorów 2 osobne sesje zdalne po min. 2 dni, dla łącznie 4 osób, należy uwzględnić min. 14 dni odstępu między szkoleniami

Dokumentacja powykonawcza, procedury zarządzania usługami katalogowymi

Stabilizacja rozwiązania wsparcie 10 h prze 3 miesiące

Przykładowa agenda szkolenia

Usługi Active Directory Services w Windows Server

1. Zaawansowane wdrażanie i administrowanie AD DS

a) Wdrażanie usług AD DS

b) Wdrażanie i klonowanie wirtualnych kontrolerów domeny

c) Wdrażanie kontrolerów domeny w systemie Windows Azure

d) Administrowanie AD DS

2. Zabezpieczanie AD DS

a) Zabezpieczanie kontrolerów domeny

b) Wdrażanie bezpieczeństwa konta

c) Wdrażanie uwierzytelnienia kontroli

3. Wdrażanie i administrowanie lokacjami AD DS i replikacją

a) Omówienie replikacji usług AD DS

b) Konfigurowanie witryn AD DS

c) Konfigurowanie i monitorowanie replikacji usług AD DS

4. Wdrażanie zasad grupy

a) Wprowadzenie do zasad grupy

b) Wdrażanie i administrowanie obiektami GPO

c) Zakres zasad grupy i przetwarzanie zasad grupy

d) Rozwiązywanie problemów z zastosowaniem obiektów zasad grupy

5. Zarządzanie ustawieniami użytkownika za pomocą zasad grupy

a) Wdrażanie szablonów administracyjnych

b) Konfigurowanie przekierowania folderu i skryptów

c) Konfigurowanie preferencji zasad grupy

6. Wdrażanie i zarządzanie usługami AD CS

a) Wdrażanie urzędów certyfikacji

b) Administrowanie urzędami certyfikacji

c) Rozwiązywanie problemów, utrzymanie i monitorowanie urzędów certyfikacji

7. Wdrażanie i zarządzanie certyfikatami

a) Korzystanie z certyfikatów w środowisku biznesowym

b) Wdrażanie i zarządzanie szablonami certyfikatów

c) Zarządzanie wdrażaniem, unieważnianiem i odzyskiwaniem certyfikatów

d) Wdrażanie i zarządzanie kartami inteligentnymi

8.Monitorowanie, zarządzanie i odzyskiwanie usług AD DS

a) Monitorowanie AD DS

b) Zarządzanie bazą danych AD DS

c) Opcje tworzenia kopii zapasowych i odzyskiwania AD DS oraz innych rozwiązań w zakresie tożsamości i dostępu

9.Wdrażanie i zarządzanie AD LDS

a) Przegląd AD LDS

b) Wdrażanie usług AD LDS

c) Konfigurowanie wystąpień i partycji AD LDS

d) Konfigurowanie replikacji usług AD LDS

e) Integracja AD LDS z AD DS

## Zasilacze awaryjne UPS – 9 szt.

Moc pozorna 1500 VA

Moc rzeczywista 1000 W

Maks. czas przełączenia na baterię maks. 10 ms

Architektura UPSa Line-interactive

Czas podtrzymania dla obciążenia 100% min. 6 min

Czas podtrzymania przy obciążeniu 50% min. 24 min

Zimny start Tak

Typ gniazda wejściowego IEC320 C14 (10A)

Liczba i rodzaj gniazdek z utrzymaniem zasilania 4 x IEC320 C13 (10A)

Układ automatycznej regulacji napięcia (AVR) Tak

Sinus podczas pracy na baterii Tak

Porty komunikacji szeregowy (forma RJ-45), USB

Wyposażenie Kabel USB, Elementy montażowe do szafy RACK

Format: RACK 2U

Wartość znamionowa udaru energii 459 J

Tryby alarmu dźwiękowego Alarm kiedy pracuje na baterii, Alarm niskiego stanu akumulatora

Akumulatory wymieniane podczas pracy Tak (hot-swap, możliwa samodzielna wymiana przez użytkowna)

Automatyczny test baterii Tak

Zimny start Tak

Wyświetlacz LCD z możliwością podglądu statusu i parametrów pracy oraz danych urządzenia, w tym datę ostatniej wymiany baterii.

Możliwość wykonania:

• UPS Self Test

• UPS Alarms Test

• Calibration Test

Gwarancja 2 lata.

W komplecie karta do zdalnego monitorowania i sterowania indywidualnym zasilaczem UPS poprzez bezpośrednie podłączenie go do sieci, obsługa HTTPS/SSL, SSH (up to 2048-bit encryption), SNMPv3, IPv4/IPv6. Pozwala skonfigurować powiadomienia o problemach. Dla chronionych serwerów umożliwia zdalne wyłączenie serwera. Kartę należy uwzględnić w cenie UPSa.

Akcesoria dodatkowe:

- kabel zasilający C13 / C14 – 5 m, - 1 szt.

- kabel zasilający adapter C14 do Schuko F – 10-30 cm, - 1 szt.

- listwa zasilająca 19", 9 gniazd, z wyłącznikiem, przewód 3m - przekrój przewodów 1,5mm2, rodzaj gniazd: CEE 7/5 (typu "francuskiego"), DIN 49440, rodzaj wtyku: CEE 7/7 ("Unischuko"), DIN 49441

- patchcord S/FTP kat.6A PiMF 2x RJ45 linka – 3 m – 1 szt.

Wyposażenie dodatkowe nie musi pochodzić od producenta UPS, gwarancja 12 mies., należy uwzględnić w cenie UPSa.

## Oprogramowanie do wirtualizacji

Zamawiający wskazuje oprogramowanie VMware vSphere 7 Essentials Plus Kit for 3 hosts (obowiązuje dla min. 3 serwerów dwuprocesorowych) wraz z min. 1 licencją vCenter Server Essentials oraz z subskrypcją na 3 lata lub równoważne. Licencja niewyłączna i nieograniczona czasowo.

Dla oprogramowania musi być publicznie znany cykl życia przedstawiony przez producenta systemu i dotyczący rozwoju wsparcia technicznego – w szczególności w zakresie bezpieczeństwa. Wymagane jest prawo do instalacji aktualizacji i poprawek do danej wersji oprogramowania, udostępnianych przez producenta na jego stronie internetowej w okresie co najmniej 3 lat.

Warunki równoważności oprogramowania dla środowisk wirtualnych

1. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych

2. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.

3. Licencja na oprogramowanie do wirtualizacji musi dostarczać możliwość uruchomienia oprogramowania na co najmniej 3 serwerach fizycznych dwuprocesorowych,

4. Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania zarówno, jako aplikacja na maszynie fizycznej lub wirtualnej, jak i jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. Virtual appliance.

5. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.

6. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.

7. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.

8. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku.

9. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.

10. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.

11. Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.

12. Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn.

13. Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych.

14. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie.

15. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA) , aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.

16. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.

17. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).

18. Oprogramowanie musi mieć możliwość instalacji na dedykowanej pamięci typu flash.

Wymagana jest możliwość przekierowania fizycznego portu USB serwera do konkretnej maszy wirtualnej.

Wdrożenie oprogramowania w zakresie min.:

Instalacja hypervizora na 3 hostach

Aktualizacja hypervizora

Konfiguracja hypervizora

Podłączenie data store

Instalacja centralnego serwera VMware vCenter for Essentials

Konfiguracja serwera centralnego zarządzania

Konfiguracja ustawień sieciowych

Utworzenie klastra vSphere Essentials

Połączenie hostów VMware ESXi z serverem VMware vCenter

Konfiguracja Virtual Switch dla ruchu maszyn wirtualnych

Test z wykorzystaniem maszyny wirtualnej

Przeprowadzenie szkolenia technicznego

Szkolenie odbędzie się zdalnie - wideokonferencja.

Czas trwania szkolenia – min. 4h.

Szkolenie poprowadzi inżynier biorący udział we wdrażaniu.

Szkolenie przeznaczone będzie dla administratorów wdrożonego rozwiązania.

Liczba osób mogąca uczestniczyć w szkoleniu: 4.

Zakres szkolenia będzie zgodny z wdrożonym rozwiązaniem.

Opracowanie dokumentacji technicznej zawierającej:

Przedstawienie konfiguracji wdrożonego rozwiązania.

Wykaz uprawnień i kont.

Lista zmian wprowadzonych w środowisku.

# Część 3 – dostawa komputerów, laptopów, peryferii i akcesoriów, oprogramowania

Komputery standardowe oraz stacje robocze wraz z monitorami powinny pochodzić od jednego producenta w celu uproszczenia wdrażania, zarządzania i utrzymania. Długość gwarancji na komputer musi być taka sama jak długość gwarancji na monitor.

## Zestaw komputerowy standardowy – 45 szt.

Zestaw komputerowy składający się z komputera standardowego i monitora standardowego o parametrach:

### komputer standardowy – 45 szt.

|  |  |  |  |
| --- | --- | --- | --- |
| **Nazwa komponentu** | | **Wymagane parametry** | |
| Zastosowanie | | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna | |
| Procesor | | Procesor klasy x86, min. 6 rdzeniowy, osiągający w teście PassMark CPU Mark wynik min. 13500 punktów na dzień 21.03.2023 r. (wynik zaproponowanego procesora musi znajdować się na stronie  <http://www.cpubenchmark.net>) | |
| Pamięć operacyjna RAM | | min. 8GB DDR4, możliwość rozbudowy do min. 32GB | |
| Parametry pamięci masowej | | min. 256GB SSD M.2 NVMe PCIe, | |
| Wydajność grafiki | | Grafika zintegrowana z procesorem powinna umożliwiać pracę dwumonitorową z wsparciem DirectX 12 OpenGL 4.5, pamięć współdzielona z pamięcią RAM, | |
| Wyposażenie multimedialne | | Min 24-bitowa Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik w obudowie komputera. | |
| Obudowa | | Typu Small Form Factor z obsługą kart PCI Express low profile  Suma wymiarów obudowy nie może przekraczać 80 cm, waga max 5 kg,  Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń bez konieczności użycia narzędzi.  Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (śrub motylkowych).  Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) oraz kłódki (oczko w obudowie do założenia kłódki).  Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS. | |
| Bezpieczeństwo | | Wbudowany (nie dopuszcza się zintegrowanych z płytą główną tzn. układ wykorzystujący jakiekolwiek złącza wyprowadzone na płycie) w płycie głównej dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. | |
| 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). | |
| BIOS | | * BIOS zgodny ze specyfikacją UEFI, pełna obsługa BIOS za pomocą klawiatury. Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący  utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS) * Funkcja blokowania/odblokowania BOOT-owania stacji  roboczej z zewnętrznych urządzeń * Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na poziomie systemu, administratora oraz dysku Możliwość włączenia/wyłączenia zintegrowanej karty dźwiękowej, karty sieciowej, portu  równoległego, portu szeregowego z poziomu BIOS, bez uruchamiania systemu operacyjnego z dysku twardego  komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. * Możliwość wyłączania portów USB | |
| Certyfikaty i standardy | | * produkowany zgodnie z normami ISO 9001 * posiada deklarację zgodności CE * spełnia kryteria środowiskowe, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki lub wykonawcy (wg wytycznych Krajowej Agencji Poszanowania Energii S.A.,  zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych  o masie powyżej 25 gram * jest produkowany zgodnie z normami Energy Star 6.1 * opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu. | |
| Ergonomia | | Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy IDLE wynosząca maksymalnie 27,5 dB | |
| Warunki gwarancji | | min. 24-miesięczna gwarancja producenta świadczona na miejscu u klienta,  W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego.  Czas reakcji serwisu - do końca następnego dnia roboczego, do godz.16.00. Gwarancja musi oferować przez cały okres :  - usługi serwisowe świadczone w miejscu instalacji urządzenia  - dostępność wsparcia technicznego przez 24 godziny 7 dni  w tygodniu przez cały rok (w języku polskim w dni robocze)   - dostęp do portalu technicznego producenta, który umożliwi  zamawianie części zamiennych i/lub wizyt technika serwisowego, mający na celu przyśpieszenie i procesu  diagnostyki i skrócenia czasu usunięcia usterki  - w przypadku wystąpienia usterki wsparcie techniczne ma  Rozwiązywać problemy z fabrycznie zainstalowanym oprogramowaniem  - w przypadku wystąpienia usterki wymagana jest natychmiastowa  reakcja wsparcia technicznego (diagnostyka zaraz po wystąpieniu awarii)  Serwis urządzeń musi być realizowany przez Producenta lub  Autoryzowanego Partnera Serwisowego Producenta. | |
| Wsparcie techniczne producenta | | Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej  komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.  Dostęp do najnowszych sterowników i uaktualnień na stronie  producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera. | |
| System operacyjny | | Zainstalowany Microsoft Windows 10 Professional PL - 64 bit lub  równoważny, o parametrach równoważności podanych poniżej.  Zainstalowany system operacyjny nie wymagający już aktywacji za pomocą telefonu lub Internetu w firmie producenta oprogramowania.  Parametry równoważności: Pełna integracja z domeną Active Directory  MS Windows opartą na serwerach Windows Server 2021; Zarządzanie komputerami poprzez Zasady Grup (GPO) Active Directory MS Windows  Zamawiającego), WMI; Zainstalowany system operacyjny nie wymaga  aktywacji za pomocą telefonu lub Internetu; Pełna integracja Płatnik ZUS; Pełna obsługa ActiveX  Wszystkie w/w funkcjonalności nie mogą być realizowane z zastosowaniem wszelkiego rodzaju emulacji i wirtualizacji. | |
|  | |
|  | |
|  | |
|  | |
|  | |
|  | |
|  | |
|  | |
|  | |
| Zarządzanie | | Możliwość zmiany stanu zasilania (zdalne wyłączanie i uruchamianie, Podpięcie zdalnych nośników masowych (np. obrazu ISO), KVM  również zdalne  uruchamianie | |
| Wyposażenie | | Przewód zasilający, klawiatura, mysz | |
| Wyposażenie dodatkowe | | patchcord RJ45 CAT 6A S/FTP Cu, LS1ZH, 3m (+/-10%) | |
| Wbudowane porty: | | * min. 2 cyfrowe złącza video, min. 1x DisplayPort; | |
|  | | * min. 8 portów USB wyprowadzonych na zewnątrz komputera, w tym min. 2 porty USB 3.2 Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. | |
|  | | * uniwersalny port słuchawek i mikrofonu na przednim panelu obudowy. | |
|  | | * karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika), PXE 2.1, * płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki dedykowana dla danego urządzenia; wyposażona w: | |
|  | | * min. 1 wolne złącze PCI Express x16 low profile, * klawiatura USB w układzie polski programisty | |
|  | | * mysz optyczna USB z trzema klawiszami oraz rolką (scroll) | |
|  | | * nagrywarka DVD +/-RW | |

### monitor standardowy – 45 szt.

|  |  |
| --- | --- |
| Przekątna matrycy | 23,0" |
| Standard matrycy | Full HD |
| Rozdzielczość matrycy | 1920 x 1080 |
| Powłoka matrycy | Matowa |
| Technologia ekranu | IPS |
| Jasność matrycy | 250 cd/m2 |
| Czas reakcji matrycy | 5 ms |
| Częstotliwość odświeżania matrycy | 60 Hz |
| Kąt widzenia pionowy | 178 stopni |
| Kąt widzenia poziomy | 178 stopni |
| Display Port | 1 szt |
| HDMI | 1 szt |
| USB | 4 szt |
| Zasilanie | Zasilacz wbudowany |
| Rodzaj gwarancji | Next Bussines Day Basic (Naprawa u klienta) |
| Czas trwania gwarancji | 24 miesiące |
| Funkcje monitora | Montaż na ścianie (VESA), Możliwość pochylenia panela (tilt), Obrotowa podstawa monitora (swivel), Panel obrotowy (pivot), Regulacja wysokości monitora (height adjustment) min 110 mm |
| Typ stojaka | Monitor stand |
| Akcesoria | Kabel zasilający, kabel DP, kabel USB |
| Opcje | Wymagana jest możliwość osobnego zakupu dedykowanego soundbara do integracji z monitorem |

## Laptop – 35 szt.

|  |  |
| --- | --- |
| Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna |
| Procesor | 4 rdzenie, wydajność w teście Passmark CPU Mark na dzień 21.03.2023 r. min. 9 900 pkt, Single Thread Rating min 2 700 pkt |
| Karta graficzna | zintegrowana z procesorem |
| Pamięć RAM | 8 GB |
| Dysk | SSD M.2 PCIe 256 GB |
| Typ ekranu | Matowy, LED, 15,6" 1920 x 1080 |
| Jasność matrycy | 250 cd/m² |
| Multimedia | Kamera internetowa, mikrofon, głośniki |
| Łączność | LAN 1 Gb/s, WiFi 6, Bluetooth 5.0 |
| Gniazda USB | 3x typu A - ilość portów fizycznych (bez stosowania przelotek lub rozgałęziaczy), 1x Thunderbolt |
| Układ klawiatury | QWERTY, wydzielona klawiatura numeryczna |
| Układ TPM | Tak, 2.0 |
| Waga | maks. 2 kg |
| System operacyjny | Microsoft Windows 10 Pro PL (wersja 64-bitowa) |
| Gwarancja | 24 miesiący (gwarancja producenta na terenie Polski), Next Business Day on site, kupujący zachowuje dysk twardy w przypadku jego awarii |
| Wyposażenie | zasilacz |
| Wyposażenie dodatkowe | Torba z osobną kieszenią na akcesoria sygnowana logiem producenta laptopa,  Mysz optyczna USB 2 przyciski z rolką, czarna, 1200DPI  patchcord RJ45 CAT 6A S/FTP Cu, LSZH, 3 m (+/-10%) |
| Wytrzymałość | Standard militarny MIL-STD-810H |

## Zaawansowana stacja robocza – 4 szt.

Zaawansowana stacja robocza składająca się ze stacji roboczej i dwu monitorów zaawansowanych o parametrach:

### stacja robocza – 4 szt.

|  |  |  |  |
| --- | --- | --- | --- |
| **Nazwa komponentu** | | **Wymagane parametry** | |
| Zastosowanie | | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna | |
| Procesor | | Procesor klasy x86, min. 8 rdzeniowy, osiągający w teście PassMark CPU Mark wynik min. 17 000 punktów na dzień 21.03.2023 r. (wynik zaproponowanego procesora musi znajdować się na stronie  <http://www.cpubenchmark.net>) | |
| Pamięć operacyjna RAM | | min. 8GB DDR4, możliwość rozbudowy do 64GB, | |
| Parametry pamięci masowej | | min. 512GB SSD M.2 NVMe PCIe,, ogółem 2 złącza M.2 dla dysków SSD | |
| Wydajność grafiki | | Grafika zintegrowana z procesorem powinna umożliwiać pracę dwumonitorową z wsparciem DirectX 12 OpenGL 4.5, pamięć współdzielona z pamięcią RAM, | |
| Wyposażenie multimedialne | | Min 24-bitowa Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik w obudowie komputera. | |
| Obudowa | | Typu Small Form Factor z obsługą kart PCI Express low profile  Suma wymiarów obudowy nie może przekraczać 70 cm, waga max 5,5 kg,  Moduł konstrukcji obudowy w jednostce centralnej komputera  powinien pozwalać na demontaż kart rozszerzeń bez konieczności użycia narzędzi.  Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów).  Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) oraz kłódki (oczko w obudowie do założenia kłódki).  Obudowa musi być wyposażona w zamek szybkiego dostępu który nie wystaje poza obrys obudowy i musi być usytuowany na bocznym panelu.  Każdy komputer powinien być oznaczony niepowtarzalnym  numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS. | |
| Bezpieczeństwo | | Wbudowany (nie dopuszcza się zintegrowanych z płytą główną tzn. układ wykorzystujący jakiekolwiek złącza wyprowadzone na płycie) w płycie głównej dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. | |
| 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). | |
| BIOS | | * BIOS zgodny ze specyfikacją UEFI, pełna obsługa BIOS za pomocą klawiatury. Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący  utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS) * Funkcja blokowania/odblokowania BOOT-owania stacji  roboczej z zewnętrznych urządzeń * Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na poziomie systemu, administratora oraz dysku Możliwość włączenia/wyłączenia zintegrowanej karty dźwiękowej, karty sieciowej, portu  równoległego, portu szeregowego z poziomu BIOS, bez uruchamiania systemu operacyjnego z dysku twardego  komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. * Możliwość wyłączania portów USB | |
| Certyfikaty i standardy | | * produkowany zgodnie z normami ISO 9001 * posiada deklarację zgodności CE * spełnia kryteria środowiskowe, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki lub wykonawcy (wg wytycznych Krajowej Agencji Poszanowania Energii S.A.,  zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych  o masie powyżej 25 gram * jest produkowany zgodnie z normami Energy Star 6.1 * opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu. | |
| Warunki gwarancji | | min. 24-miesięczna gwarancja producenta świadczona na miejscu u klienta,  W przypadku awarii dysków twardych, dysk pozostaje  u Zamawiającego.  Czas reakcji serwisu - do końca następnego dnia roboczego, do godz.16.00. Gwarancja musi oferować przez cały okres :  - usługi serwisowe świadczone w miejscu instalacji urządzenia  - dostępność wsparcia technicznego przez 24 godziny 7 dni  w tygodniu przez cały rok (w języku polskim w dni robocze)   - dostęp do portalu technicznego producenta, który umożliwi  zamawianie części zamiennych i/lub wizyt technika  serwisowego, mający na celu przyśpieszenie i procesu  diagnostyki i skrócenia czasu usunięcia usterki  - w przypadku wystąpienia usterki wsparcie techniczne ma  rozwiązywać problemy z fabrycznie zainstalowanym  oprogramowaniem  - w przypadku wystąpienia usterki wymagana jest natychmiastowa  reakcja wsparcia technicznego (diagnostyka zaraz po wystąpieniu awarii)  Serwis urządzeń musi być realizowany przez Producenta lub  Autoryzowanego Partnera Serwisowego Producenta. | |
| Wsparcie techniczne producenta | | Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej  komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.  Dostęp do najnowszych sterowników i uaktualnień na stronie  producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera .. | |
| System operacyjny | | Zainstalowany Microsoft Windows 10 Professional PL - 64 bit lub  równoważny, o parametrach równoważności podanych poniżej.  Zainstalowany system operacyjny nie wymagający już aktywacji za pomocą telefonu lub Internetu w firmie producenta oprogramowania.  Parametry równoważności: Pełna integracja z domeną Active Directory  MS Windows opartą na serwerach Windows Server 2021; Zarządzanie komputerami poprzez Zasady Grup (GPO) Active Directory MS Windows , WMI; Zainstalowany system operacyjny nie wymaga  aktywacji za pomocą telefonu lub Internetu; Pełna integracja Płatnik ZUS; Pełna obsługa ActiveX  Wszystkie w/w funkcjonalności nie mogą być realizowane z zastosowaniem wszelkiego rodzaju emulacji i wirtualizacji. | |
|  | |
|  | |
|  | |
|  | |
|  | |
|  | |
|  | |
|  | |
|  | |
| Zarządzanie | | Możliwość zmiany stanu zasilania (zdalne wyłączanie i uruchamianie, Podpięcie zdalnych nośników masowych (np. obrazu ISO), KVM  również zdalne  uruchamianie | |
| Inne | | WI-FI 6, Bluetooth 5 | |
| Zasilacz | | 80Plus bronze | |
| Wyposażenie | | Przewód zasilający,  bezprzewodowe klawiatura w układzie polski programisty i mysz | |
| Wyposażenie dodatkowe | | patchcord RJ45 CAT 6A S/FTP Cu, LSZH, 3m (+/-10%) | |
| Wbudowane porty: | | * min. 2 x DisplayPort; | |
|  | | * min. 8 portów USB wyprowadzonych na zewnątrz komputera, w tym min. 2 porty USB 3.2 po jednym USB 3.2 Gen 2 Type-A i Type-C na przednim panelu. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. | |
|  | | * uniwersalny port słuchawek i mikrofonu na przednim panelu obudowy. | |
|  | | * karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika), PXE 2.1, * płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki dedykowana dla danego urządzenia; wyposażona w: | |
|  | | * min. 1 wolne złącze PCI Express x16, * 2x M.2-2280, 1x M.2-2230 | |
|  | |  | |
|  | | * nagrywarka DVD +/-RW | |

### monitor zawansowany – 8 szt.

Informacje podstawowe

Zastosowanie Do domu i biura

Przekątna ekranu 27"

Rozdzielczość 2560 x 1440 (WQHD)

Format 16:9

Ekran Płaski

Specyfikacja

Powłoka matrycy Matowa

Typ matrycy IPS

Rodzaj podświetlenia LED / WLED

Czas reakcji maksymalnie 8 ms

Jasność minimum 350 cd/m2

Kąt widzenia (poziomy/pionowy) 178°/178°

Liczba wyświetlanych kolorów 16.7 mln

Technologia ochrony oczu Redukcja migotania, Redukcja niebieskiego światła

Złącza

1x HDMI (HDCP 1.4)

1x DisplayPort 1.4 (HDCP 1.4)

1x DisplayPort output (HDCP 1.4)

1x USB-C (wspiera DisplayPort 1.4 i Power Delivery do 90W)

4x USB 3.2 Gen 1 downstream

Obrotowy ekran (PIVOT) Tak

Możliwość montażu na ścianie (VESA) Tak

Regulacja wysokości Tak

Gwarancja 2 lata

Akcesoria:

kabel DisplayPort

kabel USB

kabel zasilający

Zasilacz wbudowany, wydajność energetyczna na poziomie EPEAT® Gold

## Drukarka igłowa – 1 szt.

Drukarka 9-igłowa, 10” wraz z kablem

|  |  |
| --- | --- |
|  |  |
| 1.1 | szybkość druku Draft: 10 cpi: 260 znaków/s, |
| 1.2 | rozdzielczość 240 x 144 dpi |
| 1.3 | Pamięć buforowa drukarki nie mniej niż 100kB |
| 1.4 | Emulacja ESC/P, IBM PPDS |
| 1.5 | Trwałość głowicy: min 350 uderzeń/igłę |
| 1.6 | Złącza: równoległy Centronics, USB 2.0, RS-232 |
| 1.7 | Rodzaj nośnika Możliwość druku na składance, pojedynczych kartkach i kopertach |
| 1.8 | Drukowanie na papierze wielowarstwowym oryginał+4 kopie |
| 1.9 | Gwarancja 36 miesięcy od dnia odbioru końcowego |
| 1.10 | Kabel Centronics o długości od 1,5m do 2m |

## Tester sieciowy 10G z obsługą PoE

Urządzenie do weryfikacji i serwisowania okablowania do transmisji głosu, obrazu oraz danych.

Możliwości:

Szybko określa czy problem jest spowodowany przez zły lub niepodłączony kabel, niewystarczające zasilanie lub urządzenie zasilające.

Informacja dla inżyniera sieci w celu zbadania potencjalnej konfiguracji switcha lub nieprawidłowego działania.

Określanie czy port może zapewnić wystarczającą moc, raportując klasę PoE (0-8).

Graficzna identyfikacja zasilanych par. Zawiera podwójny podpis, gdzie port zapewnia zasilanie 2 lub 4 par (802.3bt lub PoE ++), wyświetla poziom napięcia.

Określa czy kabel jest podłączony do portu switcha i prędkość portu do 10G.

Testowanie kabla –zwarte, otwarte lub skrzyżowane przewody na obu końcach, długość każdej pary, Generator tonów do wyszukiwania kabli.

Graficzna mapa połączeń, długość, identyfikator kabla i odległość do błędu wyświetlane na jednym ekranie.

Testuje wszystkie popularne typy przewodów, w tym RJ11, RJ45, bez potrzeby stosowania adapterów.

Śledź praktycznie każdą parę kabli lub przewodów za pomocą tonowania cyfrowego i analogowego.

Sprawdza dzisiejsze usługi multimedialne, w tym Ethernet 10/100/1000, POTS i PoE.

Podświetlany wyświetlacz LCD.

Pasek magnetyczny do przymocowania do szafy metalowej.

Zakres dostawy

Urządzenie testujące ze zdalnym adapterem

Sonda do identyfikacji przewodów

Zdalne identyfikatory RJ45 – 6 szt.

Kabel krosowy (ekranowany RJ45 i RJ11)

Baterie

Uchwyt magnetyczny

Walizka

## Oprogramowanie biurowe – 55 licencji

**Microsoft Office Home & Business 2021 lub równoważny pakiet biurowy**

Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Dostępność pakietu w wersjach 32-bit oraz 64-bit umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej.
2. Wymagania odnośnie interfejsu użytkownika:
3. a. Pełna polska wersja językowa interfejsu użytkownika.
4. b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.

3. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:

1. Posiada kompletny i publicznie dostępny opis formatu.
2. Ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2

Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

1. Pozwala zapisywać dokumenty w formacie XML.

4. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb Zamawiającego.

5. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).

6. Do aplikacji pakietu musi być dostępna pełna dokumentacja w języku polskim.

7. Pakiet zintegrowanych aplikacji biurowych musi zawierać:

1. Edytor tekstów.
2. Arkusz kalkulacyjny.
3. Narzędzie do przygotowywania i prowadzenia prezentacji.
4. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami).

8. Edytor tekstów musi umożliwiać:

1. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
2. Wstawianie oraz formatowanie tabel.
3. Wstawianie oraz formatowanie obiektów graficznych.
4. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).
5. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.
6. Automatyczne tworzenie spisów treści.
7. Formatowanie nagłówków i stopek stron.
8. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.
9. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
10. Określenie układu strony (pionowa/pozioma), niezależnie dla każdej sekcji dokumentu.
11. Wydruk dokumentów.
12. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.
13. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2007 lub Microsoft Word 2010, 2013, 2016, 2019, 2021 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.
14. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
15. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem.
16. Wymagana jest dostępność mechanizmów umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.

9. Arkusz kalkulacyjny musi umożliwiać:

1. Tworzenie raportów tabelarycznych.
2. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych.
3. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
4. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML).
5. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych.
6. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych.
7. Wyszukiwanie i zamianę danych.
8. Wykonywanie analiz danych przy użyciu formatowania warunkowego.
9. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.
10. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
11. Formatowanie czasu, daty i wartości finansowych z polskim formatem.
12. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
13. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2007 oraz Microsoft Excel 2010, 2013, 2016, 2019, 2021, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
14. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

10. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:

1. Przygotowywanie prezentacji multimedialnych, które będą:
2. Prezentowanie przy użyciu projektora multimedialnego.
3. Drukowanie w formacie umożliwiającym robienie notatek.
4. Zapisanie jako prezentacja tylko do odczytu.
5. Nagrywanie narracji i dołączanie jej do prezentacji.
6. Opatrywanie slajdów notatkami dla prezentera.
7. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo.
8. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego.
9. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym.
10. Możliwość tworzenia animacji obiektów i całych slajdów.
11. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera.
12. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2007, MS PowerPoint 2010, 2013, 2016, 2019, 2021.

11. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:

1. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego.
2. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych.
3. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców.
4. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną.
5. Automatyczne grupowanie wiadomości poczty o tym samym tytule.
6. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy.
7. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów.
8. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie.
9. Zarządzanie kalendarzem.
10. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników.
11. Przeglądanie kalendarza innych użytkowników.
12. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach.
13. Zarządzanie listą zadań.
14. Zlecanie zadań innym użytkownikom.
15. Zarządzanie listą kontaktów.
16. Udostępnianie listy kontaktów innym użytkownikom.
17. Przeglądanie listy kontaktów innych użytkowników.
18. Możliwość przesyłania kontaktów innym użytkowników.
19. Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http.

Oprogramowanie musi być sprzedawane po raz pierwszy – nie dopuszcza się licencji odzyskiwanych. Oprogramowanie musi być w najnowszej dostępnej wersji.

# Część 4 – dostawa aktywnych urządzeń sieciowych

W celu zapewnienia wysokiej kompatybilności i uproszczenia zarządzania wszystkie urządzenia aktywne (switche, zasilacze, wkładki SFP+) muszą pochodzić od jednego producenta.

## Przełączniki systemowe

Przełączniki systemowe muszą umożliwiać zarządzanie jako stack składający się z co najmniej 8 switchy.

Każdy przełącznik systemowy należy wyposażyć w

- nadajnik-odbiornik SFP+, 10GBase dla światłowodu jednomodowego 9/125µm – 2 szt.,

Wyposażenie dodatkowe dla przełączników systemowych:

- patchcord światłowodowy jednomodowy 9/125µm LC duplex 5 m – 2 szt.

- patchcord S/FTP kat.6A PiMF 2x RJ45 linka 5 m – 2 szt.,

- patchcord S/FTP kat.6A PiMF 2x RJ45 linka 1 m – 10 szt.,

- patchcord S/FTP kat.6A PiMF 2x RJ45 linka 2 m – 30 szt.,

- przewód zasilający IEC C14 - IEC C13 5 m – 1 szt.,

- przewód zasilający wtyk uniwersalny (DIN49441) - IEC C13 3 m – 1 szt.,

- organizer kabli do szaf rack 19”, grzebieniowy, min. 20 uchwytów, kolor czarny, stalowy panel, osłona na kable, zestaw montażowy (4 śruby M6 z koszyczkami) – 2 szt.,

- organizer kabli 80x80 (haczyk), metal, umożliwiający uporządkowanie i umocowanie okablowania ułożonego poziomo w szafie – 2 szt.

Wyposażenie dodatkowe nie musi pochodzić od producenta pozycji głównej, jeśli nie określono inaczej gwarancja na te pozycje wynosi 12 miesięcy. Wyposażenie dodatkowe należy uwzględnić w cenie pozycji głównej). Tolerancja długości +/- 10%

### Switch 48 port – 2 szt.

Wymaga się aby urządzenie było objęte ograniczoną wieczystą gwarancją (do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta 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.

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

* Ilość portów 48 porty 1GBaseT, 2 x SFP+ oraz 2 x 10GBaseT niezależne
* Chłodzenie od przodu do tyłu obudowy
* Możliwość instalacji redundantnego zasilacza
* Tablica MAC min. 16K
* Tablica ARP/NDP min. 888
* Bufor 16Mb
* MTBF min. 578472 godzin
* Wydajność min. 130,9 Mp/s
* Przepustowość min. 176 Gb/s
* Port USB
* Port miniUSB
* Port zarządzania Out-of-band;
* Web GUI
* HTTPs
* CLI
* Telnet
* SSH
* SNMP
* MIB RSPAN
* Radius
* TACACS+
* DiffServ
* Możliwość łączenia w stos za pomocą interfejsów 10Gb/s
* Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh
* Non-stop forwarding (NSF)
* Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram
* IPv4/IPv6 Multicast filtering
* IGMPv3 MLDv2 Snooping
* ASM & SSM
* IGMPv1,v2 Querier
* Auto-VoIP
* Auto-iSCSI
* Policy-based routing (PBR)
* LLDP-MED
* Spanning Tree
* Green Ethernet
* STP
* MTP
* RSTP
* PV(R)STP
* BPDU/STRG Root Guard
* EEE (802.3az)
* GVRP/GMRP
* Q in Q,
* Private VLAN
* DOT1X
* MAB
* Captive Portal
* DHCP Snooping
* Dynamic ARP
* Inspection
* IP Source Guard
* CPU min 800 Mhz
* Min 1GB RAM
* Min 256MB Flash
* Min ilość obsługiwanych VLAN 4K
* OSPFv3 min. sąsiadów na interfejs 100
* UDLD
* LLPF
* DHCPv6 Snooping
* wysyłanie alertów na email
* MMRP
* Ilość ACL min. 100
* Ilość reguł na listę min. 1023 na wejściu i 511 na wyjściu
* Zasilacz z certyfikatem 80+
* 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
* FCC: 47 CFR FCC Part 15, Class A, ANSI C63.4:2014
* ISED: ICES-003:2016 Issue 6, Class A, ANSI C63.4:2014
* BSMI: CNS 13438 Class A

### Switch 48 port PoE – 3 szt.

Wymaga się aby urządzenie było objęte ograniczoną wieczystą gwarancją (do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta 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.

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

* Ilość portów 48 porty PoE+ 1GBaseT, 2 x SFP+ oraz 2 x 10GBaseT niezależne
* Chłodzenie od przodu do tyłu obudowy
* Budżet mocy PoE: 480W
* Tablica MAC min. 16K
* Tablica ARP/NDP min. 888
* Bufor 16Mb
* MTBF min. 673207 godzin
* Wydajność min. 130,9 Mp/s
* Przepustowość min. 176 Gb/s
* Port USB
* Port miniUSB
* Port zarządzania Out-of-band;
* Web GUI
* HTTPs
* SSH
* SNMP
* MIB RSPAN
* Radius
* TACACS+
* DiffServ
* Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram
* IPv4/IPv6 Multicast filtering
* CPU min 800 Mhz
* Min 1GB RAM
* Min 256MB Flash
* Min ilość obsługiwanych VLAN 4K
* Minimalna ilość przełączników w stosie: 8
* Możliwość łączenia w stos za pomocą interfejsów 10Gb/s
* Możliwość łączenia przełączników w stos w konfiguracji: spine and leaf
* Non-stop forwarding (NSF)
* Distributed Link Aggregation (LAGs across the stack)
* Double VLAN Tagging (QoQ)
* PIM-DM (Multicast Routing - dense mode)
* PIM-DM (IPv6)
* PIM-SM (Multicast Routing - sparse mode)
* PIM-SM (IPv6)
* RIPv1
* RIPv2
* OSPFv2
* RFC 2328
* RFC 1583
* OSPFv3
* 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
* FCC: 47 CFR FCC Part 15, Class A, ANSI C63.4:2014
* ISED: ICES-003:2016 Issue 6, Class A, ANSI C63.4:2014
* BSMI: CNS 13438 Class A
* CB report / certificate IEC 60950-1:2005 (ed.2)+A1:2009+A2:2013
* UL listed (UL 1950)/cUL IEC 950/EN 60950
* CE LVD: EN 60950-1: 2006 + A11:2009 + A1:2010 + A12:2011 + A2:2013
* RCM (AS/NZS) 60950.1:2015

### Switch 8x SFP+ 8x 10GbE – 1 szt.

Wymaga się aby urządzenie było objęte ograniczoną wieczystą gwarancją (do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta 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.

* Ilość portów 8 portów SFP+ oraz 8 portów 10GBaseT niezależne
* Chłodzenie od przedu do tyłu obudowy
* Tablica MAC min. 16K
* Tablica ARP/NDP min. 888
* Bufor 16Mb
* MTBF min. 196120 godzin
* Wydajność min. 238 Mp/s
* Przepustowość min. 320 Gb/s
* Port USB
* Port miniUSB
* Port zarządzania Out-of-band;
* Web GUI
* HTTPs
* CLI
* Telnet
* SSH
* SNMP
* MIB RSPAN
* Radius
* TACACS+
* DiffServ
* Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram
* IPv4/IPv6 Multicast filtering
* IGMPv3 MLDv2 Snooping
* ASM & SSM
* IGMPv1,v2 Querier
* Auto-VoIP
* Auto-iSCSI
* Policy-based routing (PBR)
* LLDP-MED
* Spanning Tree
* Green Ethernet
* STP
* MTP
* RSTP
* PV(R)STP
* BPDU/STRG Root Guard
* EEE (802.3az)
* GVRP/GMRP
* Q in Q,
* Private VLAN
* DOT1X
* MAB
* Captive Portal
* DHCP Snooping
* Dynamic ARP
* Inspection
* IP Source Guard
* CPU min 800 Mhz
* Min 1GB RAM
* Min 256MB Flash
* Min ilość obsługiwanych VLAN 4K
* DHCP Server min 2K rezerwacji
* sFlow
* Minimalna ilość przełączników w stosie: 8
* Możliwość łączenia w stos przełączników z dominującymi portami 10Gb/s oraz 1Gb/s
* Możliwość łączenia w stos za pomocą interfejsów 10Gb/s
* Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh
* Non-stop forwarding (NSF)
* Distributed Link Aggregation (LAGs across the stack)
* Ilość interfejsów IP 128
* Double VLAN Tagging (QoQ)
* Yes
* PIM-DM (Multicast Routing - dense mode)
* PIM-DM (IPv6)
* PIM-SM (Multicast Routing - sparse mode)
* PIM-SM (IPv6)
* RIPv1
* RIPv2
* OSPFv2
* RFC 2328
* RFC 1583
* OSPFv3
* OSPFv2 min. sąsiadów 400
* OSPFv3 min. sąsiadów 400
* OSPFv3 min. sąsiadów na interfejs 100
* UDLD
* LLPF
* DHCPv6 Snooping
* wysyłanie alertów na email
* MMRP
* Ilość ACL min. 100
* Ilość reguł na listę min. 1023 na wejściu i 511 na wyjściu

### Switch 12x SFP+ 12x 10GbE – 1 szt.

Wymaga się aby urządzenie było objęte ograniczoną wieczystą gwarancją (do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta 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.

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

* Ilość portów 12 portów SFP+ oraz 12 portów 10GBaseT niezależne
* Chłodzenie od przodu do tyłu obudowy
* Tablica MAC min. 16K
* Bufor 32Mb
* MTBF min. 192 tys. godzin
* Wydajność min. 357 Mp/s
* Przepustowość min. 480 Gb/s
* Port USB
* Port miniUSB
* Port zarządzania Out-of-band;
* Web GUI
* HTTPs
* CLI
* Telnet
* SSH
* SNMP
* MIB RSPAN
* Radius
* TACACS+
* DiffServ
* Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram
* IPv4/IPv6 Multicast filtering
* IGMPv3 MLDv2 Snooping
* ASM & SSM
* IGMPv1,v2 Querier
* Auto-VoIP
* Auto-iSCSI
* Policy-based routing (PBR)
* LLDP-MED
* Spanning Tree
* Green Ethernet
* STP
* MTP
* RSTP
* PV(R)STP
* BPDU/STRG Root Guard
* EEE (802.3az)
* GVRP/GMRP
* Q in Q,
* Private VLAN
* DOT1X
* MAB
* Captive Portal
* DHCP Snooping
* Dynamic ARP
* Inspection
* IP Source Guard
* CPU min 800 Mhz
* Min 1GB RAM
* Min 256MB Flash
* Min ilość obsługiwanych VLAN 4K
* DHCP Server min 2K rezerwacji
* sFlow
* Minimalna ilość przełączników w stosie: 8
* Możliwość łączenia w stos za pomocą interfejsów 10Gb/s SFP+ lub portów RJ45 10Gb/s za pomocą patchcord Cat6a. Porty RJ45 nie mogą być realizowane za pomocą modułów SFP+.
* Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh
* Non-stop forwarding (NSF)
* Distributed Link Aggregation (LAGs across the stack)
* Ilość interfejsów IP 128
* Double VLAN Tagging (QoQ)
* PIM-DM (Multicast Routing - dense mode)
* PIM-DM (IPv6)
* PIM-SM (Multicast Routing - sparse mode)
* PIM-SM (IPv6)
* RIPv2
* OSPFv2
* RFC 2328
* RFC 1583
* OSPFv2 min. sąsiadów 400
* OSPFv3 min. sąsiadów 400
* OSPFv3 min. sąsiadów na interfejs 100
* UDLD
* LLPF
* DHCPv6 Snooping
* wysyłanie alertów na email
* MMRP
* Ilość ACL min. 100
* Ilość reguł na listę min. 1023 na wejściu i 511 na wyjściu
* CE mark, commercial

## Przełączniki zdalne

### Switch 8p 1xPoE-PD – 15 szt.

Urządzenie powinno być objęte ograniczoną wieczystą gwarancją producenta trwającą do 5 lat po ogłoszeniu zaprzestania produkcji wraz z wymianą na następny dzień roboczy przez cały okres gwarancji. Urządzenie powinno być objęte 90 dniowym wsparciem technicznym realizowanym przez producenta oraz pomocą techniczną w formie czat przez cały okres gwarancji.

Przełącznik powinien obsługiwać następujące protokoły i standardy:

* IEEE 802.1Q
* Min. 64 VLAN
* IEEE 802.1p (CoS)
* Port-based QoS
* DSCP-based QoS
* DiffServ
* IEEE802.3ad
* IEEE 802.1s Multiple Multiple Spanning Trees Protocol (MSTP)
* IEEE 802.1ab Link Layer Discovery Protocol (LLDP)
* LLDP-MED
* SNMP v1, v2c, v3
* RFC 1213 MIB II
* RFC 1643 Ethernet Interface MIB
* RFC 1493 Bridge MIB
* RMON group 1, 2, 3, 9
* GARP,
* GVRP
* Auto-VoIP VLAN
* Auto-Voice VLAN
* Auto-Video VLAN
* MLD snooping v1, v2
* Auto denial-of-service (DoS) protection
* HTTP oraz HTTPS
* DHCP snooping
* RFC 2131 DHCP client
* IEEE 802.1x
* Zabezpieczenie portu poprzez blokowanie adresu MAC
* ACL w oparciu o MAC oraz IP
* Ochrona przed burzami broadcast, multicast oraz unicast
* IGMP Snooping v1/v2
* Zarządzanie przepustowością na wyjściu
* SNTP
* Wsparcie dla Port mirroring
* Konfiguracja poprzez web
* TACACS+ and RADIUS Support
* Syslog
* Urządzenie powinno mierz możliwość korzystania z zasilania PoE zamiast zasilacza sieciowego
* Procesor min. 500MHz
* Min. 128MB RAM
* Ilość portów 8 x 1000 Mb/s
* Metoda przekazywania ramek: Store-and-forward
* Przepustowość: 16 Gbps
* Ilość grup multicast min. 256
* Wielkość bazy MAC: 8k
* Minimalny czas pracy pomiędzy awariami (MTBF): 2388657 godzin
* Emisja hałasu: 0 dB
* Obsługa statycznego routingu
* Ilośc statycznych tras min: 32
* Max. konsumpcja energii: 5,5W
* Możliwość opcjonalnego zarządzania z poziomu chmury oraz aplikacji na telefon komórkowy
* Wymiary maksymalnie: 158mm szerokość x 101mm głębokość x 27 mm wysokość
* Emisja cieplna maksymalnie: 18,66 BTU/godzinę

### Switch 5p PoE – 4 szt.

Wymaga się aby urządzenie obsługiwało następujące funkcje, protokoły oraz spełniało następujące wymagania:

* IEEE 802.3i 10BASE-T
* IEEE 802.3u 100BASE-TX
* IEEE 802.3ab 1000BASE-T
* IEEE 802.3z 1000BASE-X
* IEEE 802.3x full-duplex
* IEEE 802.3af
* Ilość VLAN min 64
* IEEE 802.1p (CoS)
* Port-based QoS
* DSCP-based QoS
* Min. budżet PoE (63 Wat)
* Bufor min. 192 KB pamięci na urządzenie
* Min. czas pracy pomiędzy awariami (MTBF): 1164104 godzin
* Emisja hałasu: 0 dB
* Możliwość agregacji portów
* IGMP snooping (v1, v2, and v3)
* Kolejkowanie WRR
* Zarządzanie przez WWW
* Możliwość wykonania testu okablowania.
* Porty sieciowe: 5 x 10/100/1000Mb/s w tym 4 porty PoE+
* Możliwość przeładowania systemu operacyjnego bez wyłączania PoE na portach.
* Metoda przekazywania ramek: Store-and-forward
* Rozmiar obudowy 158 x 101 x 27mm
* Przepustowość min.: 10 Gbps

Urządzenie powinno być objęte 5 letnią gwarancją producenta.

### Switch 16p – 3 szt.

Urządzenie powinno być objęte wieczystą organiczną do 5 lat po ogłoszeniu EOL gwarancją producenta wraz z wymianą na następny dzień roboczy przez cały okres gwarancji. Urządzenie powinno być objęte 90 dniowym wsparciem technicznym realizowanym przez producenta oraz pomocą techniczną w formie czat przez cały okres gwarancji.

Przełącznik powinien obsługiwać następujące standardy oraz protokoły

* IEEE 802.3 10BASE-T
* IEEE 802.3u 100BASE-TX
* IEEE 802.3ab 1000BASE-T
* IEEE 802.3z 1000BASE-X
* IEEE 802.3x
* 16 x 10/100/1000 Mb/s Ethernet
* 2 x SFP

Wymagane jest aby przełącznik obsługiwał następujące protokoły

* IEEE 802.1D
* IEEE 802.1W
* IEEE 802.1S
* Auto-voice VLAN
* MAC lockdown
* SNMP v1, v2c, v3
* RFC 1213 MIB II
* RFC 1643 Ethernet Interface MIB
* RFC1493 Bridge MIB
* Jumbo Frame
* IEEE 802.1Q Tag VLAN
* Min. 128 VLAN
* IEEE 802.1p
* DSCP - L3 QoS
* Ograniczanie pasma na wejściu
* IEEE 802.3ad
* DHCP client
* Broadcast storm control
* Port mirroring (many-to-one)
* Port setting
* IGMP snooping v1/v2
* IEEE 802.1x (RAIDUS)
* TACACS+
* ACL - MAC, IP
* SNTP
* IEEE 802.1ab LLDP
* HTTP and HTTPS
* Ochrona przed DoS
* Syslog
* Ping & traceroute
* Konfiguracja przez www
* Ilość statycznych wpisów DHCP min.: 1024
* EEE802.3az
* Statyczny routing
* MLD Snooping
* Multicast VLAN Registration
* Minimum 15 routowalnych VLAN
* Min. 26 LAG oraz do 8 portów na LAG
* Możliwość opcjonalnego zarządzania z poziomu chmury oraz aplikacji na telefon komórkowy
* Przepustowość magistrali: 52 Gb/s
* Wielkość bufora: 2Mb
* Ilość adresów MAC: 16000
* MTBF min: 567680 godzin
* Emisja hałasu: 0dBA
* Maksymalny pobór energii: 17,4W
* Temp. pracy: 0-50 °C

Przełącznik musi spełniać następujące standardy elektromagnetyczne:

* CE,
* FCC Part 15 Class A,
* VCCI Class A Class A
* EN 55022 (CISPR 22) Class A
* Class A RCM
* EN 50082-1
* EN 55024CCC
* IEC 950/EN 6095

Strona celowo pozostawiona pusta.

# Część 5 – Oprogramowanie monitorujące sieć

Licencja bezterminowa na oprogramowanie do monitorowania i zarządzania siecią komputerów, które musi zawierać w sobie wszelkie niezbędne licencje umożliwiające pełną funkcjonalność bez ograniczeń czasowych oraz na ilość przechowywanych danych (poza licencją na systemy operacyjne), ze wsparciem na 6 miesięcy, zawierające funkcjonalności:

monitorowanie sieci - nielimitowana liczba urządzeń;

Inventory – sprzęt i oprogramowanie - zarządzanie 250 stacjami roboczymi;

Users – aktywność użytkowników - zarządzanie 250 stacjami roboczymi;

Dataguard – bezpieczeństwo danych - zarządzanie 250 stacjami roboczymi;

Helpdesk – system zgłoszeń, czat i zdalna pomoc;

Półroczne aktualizacje i wsparcie techniczne – konsultacje i naprawa zgłoszonych błędów.

Wykonawca zapewni wsparcie techniczne i wdrożeniowe przy instalacji i wdrożeniu programu w czasie trwania umowy, oraz przeszkoli 4 administratorów.

Poniżej opisano podstawowe funkcjonalności oprogramowania do monitorowania i zarządzania siecią komputerów. Zaproponowane rozwiązanie musi spełniać poniżej opisane wymagania:

Oprogramowanie musi posiadać budowę modułową, składać się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana jest przy użyciu szyfrowanego protokołu TLS 1.2. Moduły umożliwiają kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem.

Program musi wykorzystywać bazę danych opartą na silniku SQL (np.: PostgreSQL) dzięki czemu nie będzie objęty limitem ilości danych, baza danych jest rozwiązaniem darmowym niewymagającym dodatkowego licencjonowania.

Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., muszą być odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Musza być one również grupowane w osobnym, dedykowanym oknie. Pozwala to na, zgodne z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, objęty jest kontrolą na poziomie wybranych Administratorów – w programie można nadawać kontom administracyjnym różne poziomy dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak   
i użytkowników.

Główny Administrator ma możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. może wyłączyć możliwość zdalnej deinstalacji Agenta.

Moduł SIECI - MONITOROWANIE INFRASTRUKTURY (BEZAGENTOWO) musi obejmować serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:

* wykrywania urządzeń w sieci poprzez skanowanie ping (oraz arp-ping),
* wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci,
* wizualizacji połączeń pomiędzy urządzeniami a przełącznikami i informacji, do którego portu przełącznika podłączone jest dane urządzenie,
* serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów,
* serwerów pocztowych:
* program monitoruje zarówno serwis odbierający, jak i wysyłający pocztę,
* program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem),
* program ma możliwość wykonywania operacji testowych,
* program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa.
* monitorowania serwerów WWW i adresów URL,
* obsługi szyfrowania SSL/TLS w powiadomieniach e-mail,
* obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID,
* obsługi komunikatów syslog i pułapek SNMP,
* monitoringu routerów i przełączników wg:
* zmian stanu interfejsów sieciowych,
* ruchu sieciowego,
* podłączonych stacji roboczych – graficzna prezentacja panelu switcha,
* ruchu generowanego przez podłączone do portów stacje robocze.
* serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie,
* wydajności systemów Windows:
* obciążenie CPU,
* pamięci,
* zajętość dysków,
* transfer sieciowy.

Program musi posiadać Inteligentne Mapy i Oddziały, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz tworzą dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). Program musi posiadać również funkcję kompilatora plików MIB.

Moduł INWENTARYZACJI - program musi automatycznie gromadzić informacje o sprzęcie   
i oprogramowaniu na stacjach roboczych oraz:

* Prezentować szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.
* Obejmować m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.
* Informować o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji.
* Zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.
* Posiadać możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
* Umożliwiać odczytanie numeru seryjnego (klucze licencyjne).
* Umożliwiać automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
* Umożliwić przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
* Umożliwić utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie.
* Umożliwić wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji są logowane.
* Moduł inwentaryzacji zasobów musi umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:
* przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,
* tworzenia powiązań między zasobami a urządzeniami,
* tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak   
  i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,
* wskazania osób uprawnionych do użycia zasobów,
* definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz,
* importu danych z zewnętrznego źródła (.CSV),
* przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp.,
* tworzenia powiązań między zasobami a dokumentami w relacji 1:N,
* oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.,
* ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności,
* generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,
* generowania protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji,
* archiwizacji i porównywania audytów zasobów,
* tworzenia kodów kreskowych dla zasobów,
* drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy,
* inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej na system Android,
* inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline),
* definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”).

Dodatkowo dostępne musza być agenty inwentaryzacji na systemy Android, macOS oraz Linux.

Inwentaryzacja oprogramowania musi zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:

* Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.
* Informacje o aplikacjach używanych w organizacji.
* Tworzenie własnych wzorców aplikacji.
* Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.
* Informacje o komputerach, na których aplikacja została wykryta.
* Zarządzanie posiadanymi licencjami.
* Wskazywanie osób odpowiedzialnych za licencję.
* Wskazanie użytkowników licencji.
* Tworzenia powiązań między licencjami a dokumentami w relacji 1:N.

Rozbudowane zarządzanie licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.

Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych.

Zarządzanie posiadanymi licencjami: raport zgodności licencji.

Możliwość przypisania do programów numerów seryjnych, wartości itp.

Okna audytowe musi posiadać możliwość filtrowania elementów per oddział.

Moduł USER - w ZAKRESIE OBSŁUGI UŻYTKOWNIKÓW program musi umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:

* Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),
* Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach,
* Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność,
* Informacji o edytowanych przez użytkownika dokumentach,
* Historii pracy (cykliczne zrzuty ekranowe),
* Listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt),
* Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),
* Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków,
* Nagłówków przesyłanej poczty e-mail,
* blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla danej stacji roboczej z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. \*.domena.pl),
* blokowania ruchu na wskazanych portach TCP/IP,
* blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,
* wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia,
* przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika).

Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie.

Mechanizm blokowania uruchamiania aplikacji.

Program posiada Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych.

Moduł HELPDESK - w zakresie program musi umożliwiać realizację zdalnej pomocy użytkownikom.

W ramach kontroli stacji użytkownika musi być dostępny podgląd pulpitu użytkownika   
i możliwość przejęcia nad nim kontroli. Podczas dostępu zdalnego, zarówno użytkownik jak   
i administrator widzą ten sam ekran. Administrator w trakcie zdalnego dostępu ma możliwość zablokowania działania myszy oraz klawiatury dla użytkownika. W niniejszym module znajduje się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych, które z kolei są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Kolejną ważną funkcjonalnością musi być umożliwienie użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. Moduł ten musi zawierć również komunikator (czat), który umożliwia przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i administratorami (wraz z wyszukiwarką wiadomości oraz automatycznym oczyszczaniem historii rozmów) oraz bazę wiedzy pomagającą użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy.

Moduł pomocy zdalnej umożliwia również:

* pobieranie listy użytkowników z Active Directory,
* zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej,
* tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii   
  w folderach (do 4 poziomów kategorii),
* przypisywanie pracowników helpdesk do kategorii zgłoszeń,
* procesowanie zgłoszeń użytkowników z wiadomości e-mail,
* tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń,
* wykonywanie operacji na wielu zgłoszeniach równocześnie,
* dołączanie załączników do zgłoszeń,
* zrzuty ekranowe (podgląd pulpitu),
* dystrybucję oprogramowania przez agenty,
* dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI),
* zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku,
* możliwość skonfigurowania automatyzacji procesowania zgłoszeń,
* planowanie nieobecności pracowników helpdesk,
* obsługę umów o gwarantowanym poziomie świadczenia usług (SLA),
* generowanie raportów obsługi helpdesk,
* zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu),
* zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami),
* wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików.

System musi posiadać możliwość ochrony danych przed wyciekiem poprzez blokowanie:

• urządzeń i nośników danych. System musi mieć możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.

• urządzeń i interfejsów fizycznych: USB, FireWire, gniazd kart pamięci, dysków SATA, dysków przenośnych, napędów CD/DVD, stacji dyskietek.

• interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.

Blokownie musi dotyczyć tylko urządzeń służących do przenoszenia danych - inne urządzenia korzystające z tych interfejsów (drukarka, klawiatura, mysz itp.) muszą działać prawidłowo.

System musi zapewniać zarządzanie prawami dostępu do urządzeń:

• Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.

• Autoryzowanie urządzeń firmowych (np. szyfrowanych): pendrive’ów, dysków itp. - urządzenia prywatne są blokowane.

• Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników lub stacji roboczych.

• Centralną konfigurację poprzez ustawienie reguł (polityk) dla całej sieci lub wybranych stacji roboczych.

System musi zapewniać realizację audytu operacji na urządzeniach przenośnych:

• Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.

• Podłączenie/odłączenie urządzenia przenośnego.

**Wdrożenie**

Zamawiający oczekuje pomocy w uruchomieniu systemu polegającej na instalacji oprogramowania serwera, uruchomieniu monitoringu sieciowego dla min. 20 różnych urządzeń, wgraniu min. 20 agentów.

Wykonawca uzgodni harmonogram realizacji zadania z Zamawiającym. Zamawiający zastrzega możliwość odroczenia wdrożenia na 3 miesiące, zależnie od obłożenia pracą.

**Szkolenie administratorów**

• Szkolenie musi zostać przeprowadzone dla min. dwóch grup szkoleniowych w min. dwóch różnych terminach.

• Szkolenie może być prowadzone w formie zdalnej.

• Wymiar czasu szkolenia: minimum 14 godzin (dwa dni).

• Zakres szkolenia:

- zapoznanie z najważniejszymi funkcjonalnościami systemu;

- konfiguracja i korzystanie z poszczególnych modułów systemu;

- monitorowanie krytycznych dla organizacji urządzeń, usług i procesów;

- monitorowanie komponentów sieci, wydajności i pojemności;

- wykonanie audytu oprogramowania, plików multimedialnych;

- zarządzanie środkami trwałymi;

- monitorowanie i analiza aktywności użytkowników;

- standaryzacja i rozliczalność komunikacji pomiędzy użytkownikami a pracownikami IT;

- budowa bazy wiedzy dla pracowników;

- automatyzacja procesów związanych z obsługą zgłoszeń serwisowych;

- zarządzanie i rozliczanie nośników zewnętrznych;

- rozliczanie pracy na plikach wspólnych

Po zakończeniu szkolenia uczestnicy otrzymają certyfikat potwierdzający posiadaną wiedzę na poziomie administratora. Certyfikat musi być autoryzowany przez producenta systemu.

Strona celowo pozostawiona pusta.

# Część 6 – dostawa macierzy dyskowych sieciowych (NAS) – 2 szt.

## NAS 1:

Specyfikacja wspólna dla NAS oraz:

Pamięć RAM 64 GB

2 dyski M.2 PCIe NVMe 4.0 x4 przystosowane do pracy 24/7, niezawodność MTBF 1 500 000 godz., gwarancja 60 miesięcy (gwarancja producenta),) Zapis sekwencyjny 5000 MB/s, min. TBW > 1200 TB (min. 0.7 DWPD)

## NAS 2:

Specyfikacja wspólna dla NAS oraz:

Pamięć RAM 32 GB

## Specyfikacja wspólna dla NAS:

Obudowa typu Rack o wysokości 2U. Urządzenie dostarczone wraz z kompletem szyn umożliwiających montaż w szafie rack oraz wysunięcie urządzenia.

Zainstalowany min. jeden procesor czterordzeniowy dedykowany do pracy z zaoferowanym urządzeniem, umożliwiający osiągnięcie wyniku min. 4580 punktów dla procesorów równoważnej serii, w teście CPU PASSMARK na stronie https://www.cpubenchmark.net

System operacyjny i konfiguracja przechowywane w pamięci flash.

Dwa redundantne zasilacze min. 300W każdy.

Zainstalowane dyski 8 x 20 TB, 3,5 cala, min. 256MB cache, typu SATA 6 Gb/s., średni czas między awariami MTBF (godzin) 2 500 000, prędkość obrotowa (RPM) 7200, technika zapisywania danych: CMR, dedykowany do pracy w serwerach NAS i w systemach RAID w trybie 24/7, gwarancja producenta 5 lat,

Obsługa RAID: JBOD, RAID 0, 1, 5, 6, 10, 50, 60, obsługa hot-spare.

Możliwość podłączenia 2 dysków SSD M.2 2260/2280 NVMe PCIe 3.0 x4

Karty sieciowe: 2x1 GbE /RJ45, 2x10 GbE /RJ45

Porty USB min. 4, z tego min. 3x USB 3.2 Gen 2 (10 Gb/s) (min. 1 x Type A, min. 1 x Type C)

**Gwarancja min 2 lata. Zamawiający zachowuje dyski twarde w przypadku ich awarii.**

Gwarancja obejmuje: dostarczenie jednostki zastępczej, wymianę urządzenia lub jego części oraz robociznę Czas reakcji Gwaranta: dostarczenie jednostki zastępczej lub wymiana w następnym dniu roboczym po zgłoszeniu awarii przez Zamawiającego Miejsce realizacji gwarancji: w siedzibie Zamawiającego. W przypadku awarii dysku twardego lub dysku NVMe nośnik pozostaje u Zamawiającego.

## Wymagania ogólne:

Wspierane usługi:

Stacja monitoringu

Windows ACL

Integracja w Windows ADS

Serwer WWW

Serwer plików

Manager plików przez WWW

Funkcja Virtual Disk umożliwiająca zwiększenie pojemności serwera przy pomocy protokołu iSCSI

Replikacja w czasie rzeczywistym

Serwer RADIUS

Klient LDAP

Serwer Syslog

Wpierane protokoły CIFS, SMB, AFP, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP

Obsługa snapshotów (65 535 migawek).

Obsługa replikacji migawek na drugie urządzenie.

Obsługa maszyn wirtualnych Windows®, Linux®, UNIX®, Android™, obsługa kontenerów LXD, Docker® i Kata.

Obsługa systemu ZFS.

Wyposażenie dodatkowe (należy uwzględnić w cenie oferowanych macierzy, przewody nie muszą być dostarczone przez producenta NAS, obowiązuje gwarancja 12 miesięcy):

Przewód zasilający IEC C14 - IEC C13 3 m – 1 szt.,

Przewód zasilający wtyk uniwersalny (DIN49441) - IEC C13 3 m – 1 szt.,

Patchcord S/FTP kat.6A PiMF 2x RJ45 linka 5m – 2 szt.,

Uwaga: wyposażenie dodatkowe dotyczy każdego serwer NAS, czyli łącznie 4 patchcordy i 4 przewody zasilające.

## Wdrożenie

W ramach wdrożenia zamawiający oczekuje doradztwa w zakresie optymalnego ustawienia, konfiguracji urządzenia w środowisku zmawiającego, w tym integracji z Active Directory, uruchomienia replikacji danych oraz snapshotów z NAS 1 na NAS 2 w zakresie minimum 8 godz. pracy inżyniera.

Szkolenie administratorów – 4 osoby

Szkolenie musi zostać przeprowadzone dla min. dwóch grup szkoleniowych w min. dwóch różnych terminach, w odstępie min. 2 tygodnie. Szkolenie może być prowadzone w formie zdalnej. Wymiar czasu szkolenia: minimum 14 godzin (dwa dni).

Zakres szkolenia:

Omówienie możliwości sprzętowych i programowych urządzeń

Konfiguracja przestrzeni dyskowej

Architektura przestrzeni dyskowej urządzeń

Konfiguracja dysków i przestrzeni

Zaawansowane funkcje przestrzeni dyskowej

Przechowywanie danych

Udostępnianie, uprawnienia, zabezpieczenia

Backup danych

Chmura prywatna

Wirtualizacja

Wirtualizacja na urządzeniu

Współpraca urządzeń z hostami wirtualizacji

Kontenery

Monitoring

Monitoring stanu urządzenia

Monitoring urządzeń w sieci

Po zakończeniu szkolenia uczestnicy otrzymają certyfikat potwierdzający posiadaną wiedzę na poziomie administratora. Certyfikat musi być autoryzowany przez producenta systemu.

# Część 7 – dostawa i wdrożenie firewalla NG UTM – 2 szt. w klastrze

## Wymagania Ogólne

Dostawa 2 urządzeń typu firewall Next Generation z UTM pracujące jako klaster wysokiej dostępności. Zgodny z wymaganiami określonymi w "Rekomendacje Centrum e-Zdrowia w zakresie budowy systemów cyberbezpieczeństwa" https://ezdrowie.gov.pl/portal/artykul/zestaw-rekomendacji-w-zakresie-cyberbezpieczenstwa-w-ochronie-zdrowia Wymagania Ogólne - o ile poniża specyfikacja nie stanowi inaczej. Gwarancja i licencje na 12 miesięcy. Wymagane są zasilacze redundantne.

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

* Firewall.
* Ochrony w warstwie aplikacji.
* Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej.
3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
4. Monitoring stanu realizowanych połączeń VPN.
5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:

* 16 portami Gigabit Ethernet RJ-45.
* 8 gniazdami SFP 1 Gbps.
* 2 gniazdami SFP+ 10 Gbps.

1. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall’a obsługa nie mniej niż 1.5 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 10 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps.
6. 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.
7. 9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.

Funkcje Systemu Bezpieczeństwa:

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

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
12. Analiza ruchu szyfrowanego protokołem SSH.
13. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

Polityki, Firewall

1. 2. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. 3. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

1. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
3. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.

* Amazon Web Services (AWS).
* Microsoft Azure
* Google Cloud Platform (GCP).
* OpenStack.
* VMware NSX.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:

* Wsparcie dla IKE v1 oraz v2.
* Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19 i 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
* Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
* Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
* Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.

1. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

* Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
* Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:

* Routingu statycznego.
* Policy Based Routingu.
* Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać 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) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:

* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
* Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
* Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

* ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

a)     Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres [12] miesięcy

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres [12] miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7

System logowania i raportowania

Wymagania Ogólne

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

Interfejsy, Dysk:

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 500 GB.

Parametry wydajnościowe:

1. System musi być w stanie przyjmować minimum 1 GB logów na dzień.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

Logowanie

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:

a. Listę najczęściej wykrywanych ataków.

b. Listę najbardziej aktywnych użytkowników.

c. Listę najczęściej wykorzystywanych aplikacji.

d. Listę najczęściej odwiedzanych stron www.

e. Listę krajów , do których nawiązywane są połączenia.

f. Listę najczęściej wykorzystywanych polityk Firewall.

g. Informacje o realizowanych połączeniach IPSec.

1. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
2. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
3. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

Raportowanie

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

Korelacja logów

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:

* Malware.
* Aplikacje sieciowe.
* Email.
* IPS.
* Traffic.
* Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.

Zarządzanie

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.

a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.

1. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

Serwisy i licencje

1. System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.
2. Wsparcie: System musi być objęty serwisem producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

Wymagania dotyczące wdrożenia

1) Wymagania ogólne

• Wdrożenie nowego urządzenia ma na celu wymianę starej zapory sieciowej opartej o router Mikrotik RB1100Dx4 oraz wdrożenie nowoczesnych zabezpieczeń sieciowych.

• Wykonawca jest zobowiązany do wykonania instalacji i konfiguracji wymaganego urządzenia w dedykowanym pomieszczeniu serwerowni Zamawiającego, które jest wyposażone w niezbędną infrastrukturę sieciową, system zasilania awaryjnego i klimatyzację oraz szafę RACK przeznaczoną na wykonanie wszelkich prac instalacyjnych stanowiących przedmiot zamówienia.

2) Wymagany zakres prac wdrożeniowych

• Wykonawca jest zobowiązany do wykonania wszelkich prac instalacyjnych dla nowego urządzenia zgodnie z zaleceniami producenta i dobrymi praktykami, przeniesienia konfiguracji starej zapory sieciowej do nowego urządzenia i odtworzenia wszystkich połączeń fizycznych LAN/WAN. Przeniesienie konfiguracji powinno obejmować konfigurację LAN/WAN, w tym adresację IP urządzenia, VLAN-y, trasy dla routingu statycznego, VPN-y.

• W ramach dostarczonego systemu ochrony muszą zostać uruchomione i skonfigurowane funkcje ochrona IPS, ochrona antywirusowa/malware, kontrola aplikacji, kontrola stron www, kontrola zawartości poczty (ochrona przed spamem), ochrona przed sieciami botnet, kontrola zapytań DNS, deszyfracja SSL (inspekcja ruchu szyfrowanego).

3) Czas prowadzenia prac wdrożeniowych

• Zamawiający nie dopuszcza możliwości wyłączenia dostępu do sieci w czasie od poniedziałku do piątku w godzinach 7:00 -15:0, we wtorki i czwartki prace mogą odbywać się po 18:00.

• Prace wymagające wyłączenia elementów infrastruktury sieciowej, należy wykonywać po godzinach pracy Zamawiającego lub w weekendy. Prace takie należy uzgadniać z pracownikami Działu Informatycznego z minimum tygodniowym wyprzedzeniem.

4) Dodatkowe wymagania

• Urządzenie musi być dostarczone w stanie fabrycznie nowym, wolnym od wad technicznych, prawnych i formalnych zwłaszcza w zakresie licencji i uprawnień do aktualizacji oprogramowania. Sprzęt nie może być wcześniej zarejestrowany na żadnego innego klienta w bazie klientów producenta sprzętu.

• Zamawiający wymaga przed podpisaniem protokołu odbioru sprzętu zażądać oświadczenia producenta na podstawie numerów seryjnych, że oferowany sprzęt jest nowy i pochodzi z legalnego kanału dystrybucyjnego producenta. Jeśli sprzęt nie spełnia tych warunków Zamawiający odstąpi od umowy z winy Oferenta.

• Serwis urządzenia musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta.

• Przeprowadzenie co najmniej 2 dwudniowych szkoleń dla 4 administratorów urządzenia.

**AGENDA**  
1. Konfiguracja interfejsów;  
2. Obiekty:  
• Adresy, zakresy i grupy;  
• Usługi;  
• VIP.  
2. Użytkownicy lokalni i grupy;  
3. Podstawy routingu;  
4. Polityki bezpieczeństwa:  
• NAT  
• Profile bezpieczeństwa:  
• Antywirus;  
• Webfilering;  
• Filtr aplikacyjny;  
• IPS;  
• Ochrona poczty.  
• Mapowanie adresów.  
2. Wykrywanie urządzeń sieciowych;  
3. VPN:  
• IPsec;  
• SSL-VPN;  
4. FortiWiFi;  
5. Ogólne omówienie pozostałych produktów Fortinet.

Strona celowo pozostawiona pusta.

# Część 8 – dostawa oprogramowania do backupu

Ogólne:

* Oprogramowanie może być dostarczane w dwóch scenariuszach:
  + Cloud(Software as Service),
  + On-premise.
* Istnieje możliwość migracji w obie strony pomiędzy środowiskiem on-premise oraz cloud.
* Interfejs systemu dostępny jest w języku:
  + polskim,
  + angielskim,
* Oprogramowanie nie preferuje platformy sprzętowej, nie jest profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych,
* Oprogramowanie może być uruchomione w kontenerze docker,
* Możliwość instalacji oraz uruchomienia serwera zarządzania na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy:
  + Debian: 9+
  + Ubuntu: 16.04+
  + Fedora: 29+
  + centOS: 7+
  + RHEL: 6+
  + openSUSE: 15+
  + SUSE Enterprise Linux (SLES): 12 SP2+
  + Windows Client: 7, 8.1, 10 (1607+)
  + Windows Server: 2008 R2+,
* System wykonuje kopię własnej bazy danych, która umożliwia odtworzenie wszystkich ustawień i całej konfiguracji,
* Oprogramowanie działa w architekturze wykluczającej pojedynczy punkt awarii(awaria jednego z komponentów nie spowoduje przestoju),

Wsparcie techniczne:

* Pomoc techniczna w językach:
  + polskim,
  + angielskim.
* Materiały samopomocowe:
  + Baza wiedzy:
    - polski,
    - angielski

Zarządzanie:

* Zarządzanie całością działania systemu (backup, przywracanie)z poziomu jednej konsoli webowej,
* Zarządzanie całym systemem poprzez dashboardy,
* Gradacja uprawnień kont administratorów z poziomu panelu zarządzającego,
* System posiada wbudowane predefiniowane zadania backupowe,
* System umożliwia tworzenie zadań backupowych w oparciu o kalendarz.
* Automatyczne oraz ręczne uruchamianie kopii zapasowych zgodnie z ustalonym harmonogramem,
* Automatyczne oraz ręczne uruchamianie procesu przywracania zgodnie z ustalonym harmonogramem,
* Monitorowanie postępu działania zadania,
* Posiada system powiadamiania poprzez e-mail o zdarzeniach w następujących przypadkach:
  + Zadanie zostało zakończone pomyślnie,
  + Zadanie zostało zakończone z ostrzeżeniami,
  + Zadanie zostało zakończone z błędem,
  + Zadanie zostało anulowane,
  + Zadanie nie zostało uruchomione.
* System generuje alerty na konsoli WEB w przypadku zaistnienia określonego zdarzenia systemowego.
* Możliwość zdefiniowania okna backupowego dla każdego z zadań,
* Oprogramowanie posiada wbudowany menadżer haseł do przechowywania kluczy szyfrujących oraz poświadczeń do magazynów,
* System pozwala na klonowanie planów kopii zapasowych,
* System umożliwia reset hasła administratora w przypadku jego utraty,
* Oprogramowanie umożliwia definiowanie retencji według schematów:
  + GFS(Grandfather-Father-Son),
  + FIFO(First-In, First-Out).
* Oprogramowanie umożliwia tworzenie kont użytkowników nie będących administratorami,
* Konta użytkowników mogą być tworzone poprzez import pliku CSV,
* Oprogramowanie umożliwia tworzenie grup urządzeń,
* Oprogramowanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera(urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera(urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).
* System pozwala na zarządzanie multi-tenantowe - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.:
  + System Administrator,
  + Backup operator,
  + Restore operator,
  + Viewer.

Składowanie danych:

* Oprogramowanie jest systemem multi-storageowym i umożliwia tworzenie wielu repozytoriów danych jednocześnie,
* System umożliwia składowanie danych:
  + Lokalnie:
    - Zasób SMB,
    - Zasób NFS,
    - Zasób ISCSI,
    - Zasób S3,
    - Katalog zabezpieczonego urządzenia.
  + W chmurze:
    - Amazon Web Service,
    - Magazyn zgodny z S3,
    - Dostarczanej przez producenta.
* System pozwala na zdefiniowanie zapasowej ścieżki repozytorium, na wypadek niedostępności głównej lokalizacji,
* System oferuje mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.

Odtwarzanie:

* Odtwarzanie granularne:
  + Pojedynczych plików z kopii obrazu dysku,
  + Pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365,
* Wykorzystanie funkcjonalności Bare Metal Restore(kopii zapasowej całego dysku - łącznie z partycjami i danymi startowymi) dla odtwarzania systemu po awarii, wsparcie dostępne jest dla systemów:
  + Windows: 7+,
  + Windows Server: 2008 R2+,
* Odtwarzanie Bare metal Restore może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.
* Uruchamianie procesu Bare Metal Restore odbywa się z bootowalnej płyty CD lub pendrive’a,
* Oprogramowanie umożliwia odtwarzanie systemu w scenariuszach: P2P, P2V, V2P, V2V.
* Oprogramowanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie(VHD, VHDX, VMDK),
* Odtwarzanie zasobów plikowych bez praw dostępu(tzw. ACL),
* Odtwarzanie zasobów plikowych z prawami dostępu,
* Przywracanie plików pomiędzy systemami operacyjnymi(np. odtwarzanie danych plikowych Linux na systemie Windows),
* Odtwarzanie danych według harmonogramu,
* Przywracanie danych z określonego urządzenia/użytkownika,
* Przywracanie kopii z wybranego magazynu.
* Przywracanie danych Microsoft 365:
  + do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku:
    - pst,
    - mbox.
  + do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji),
* System posiada możliwość nieodwracalnego kasowania danych,
* Przywracanie repozytoriów GIT:
  + Przywracanie pomiędzy hostingami repozytoriów(GitHub/BitBucket),
  + przywracanie między kontami.

Backup:

* Wykonywanie pełnych, różnicowych, przyrostowych kopii zapasowych, a także backupu syntetycznego dla:
  + Systemów operacyjnych:
    - Alpine 3.10+,
    - Debian: 9+,
    - Ubuntu: 16.04+,
    - Fedora: 29+,
    - centOS: 7+,
    - RHEL: 6+,
    - openSUSE: 15+,
    - SUSE Enterprise Linux(SLES): 12 SP2+,
    - macOS: 10.13+,
    - Windows: 7, 8.1, 10(1607+),
    - Windows Server: 2008 R2+,
  + Środowisk wirtualnych:
    - Hyper-V,
    - VMware,
    - Dowolnych innych – agentowo.
  + Repozytoriów GIT:
    - GitHub,
    - Bitbucket.
* Wykonywanie pełnych, różnicowych oraz przyrostowych oraz logów transakcyjnych kopii zapasowych dla:
  + Baz danych**:**
    - Microsoft SQL,
    - MySQL,
    - PostgreSQL,
    - Firebird,
    - Dowolnych innych przez podpięcie skryptów pre/post.
* Szyfrowanie danych wykonywana po stronie stacji roboczej za pomocą algorytmu AES w trybie CBC z kluczem szyfrującym o długości:
  + 128 bit,
  + 192 bit,
  + 256 bit.
* Kompresja danych wykonywana po stronie stacji roboczej za pomocą algorytmów:
  + ZStandard,
  + LZ4.
* Oprogramowanie umożliwia zarządzanie poziomem kompresji,
* Wykonywanie kopii zapasowej otwartych plików(VSS),
* System umożliwia uruchamianie skryptów przed i po backupie,
* System umożliwia uruchamianie skryptów po wykonaniu migawki VSS,
* System umożliwia automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku błędów,
* Backup jednego oraz wielu dysków/całego systemu operacyjnego(Windows) ze wsparciem dla partycji MBR oraz GPT,
* Backup plikowy,
* Oprogramowanie realizuje funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie dyskowe,
* Oprogramowanie umożliwia konsolidację wersji kopii zapasowych,
* Oprogramowanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia,
* Oprogramowanie pozwala na automatyczne uruchomienie kopii zapasowej podczas zamykania systemu operacyjnego.
* Oprogramowanie pozwala na backup zaszyfrowanych partycji.

GIT

* Oprogramowanie zapewnia wsparcie dla repozytoriów lokalnych oraz zdalnych(dostępnych w usługach zewnętrznych),
* Oprogramowanie umożliwia zabezpieczenie metadanych repozytoriów(w zależności od zabezpieczanej usługi m.in.: issues, pull requests, actions/pipelines, wiki).

Licencjonowanie:

* Sposób licencjonowania opiera się na:
  + Ilości serwerów/endpointów- dla fizycznych urządzeń,
  + Ilości fizycznych hostów - dla środowisk wirtualnych,
  + Ilości repozytoriów - dla GIT.
* Licencje w wersji dożywotniej, powinny pozwalać na zabezpieczenie:
  + 230 stacji roboczych Windows
  + 1 fizycznego serwera Linux
  + Nielimitowanej ilości maszyn wirtualnych w obrębie 3 fizycznych hostów Vmware, bez limitu ilości procesorów oraz socketów.
* Wsparcie techniczne:
* Świadczone jest w języku polskim, bezpośrednio przez główną siedzibę producenta,
* Zapewnia dostęp do aktualizacji oprogramowania,
* Umożliwia korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego,

Szkolenia

Wykonawca przeszkoli zdalnie lub lokalnie 4 pracowników zamawiającego w zakresie administracji dostarczonym systemem. Szkolenia muszą odbyć się w dwóch turach, w postaci live webinaru, co najmniej 4 godziny.

Tematyka szkoleń musi obejmować:

* Typy kopii zapasowych, możliwe konfiguracje polityk backupu.
* Konfiguracja i zarządzanie polityką backupu.
* Ochrona serwerów i maszyn wirtualnych.
* Strategie zabezpieczania danych na wypadek ataku ransomware.
* Migracja danych i urządzeń.
* Uruchamianie systemu po awarii.
* Disaster recovery.