**Załącznik nr 3 do Zapytania ofertowego**

# SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Dotyczy zadania realizowanego pod nazwą:

**Dostawa sprzętu komputerowego w ramach realizacji projektu „Cyfrowa Gmina” ,**

finansowanego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotycząca realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00, dotyczy realizacji umowy nr 4323/2/2022.

## Część nr 1 serwer wraz z oprogramowaniem Windows Serwer – szt. 1

**Wymagania ogólne:**

**Obudowa -** Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2,5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.
Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
**Płyta główna -** Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
**Chipset -** Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
**Procesor** Zainstalowany jeden procesor min. 16-rdzeniowy, min. 2.4GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 229 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
Możliwość obsługi procesorów 32 rdzeniowych
**RAM -** Minimum 64GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
**Funkcjonalność pamięci RAM -** Minimum 64GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
**Funkcjonalność pamięci RAM -** Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing
**Gniazda PCI** - minimum jeden slot PCIe x16 generacji 4

**Interfejsy sieciowe/FC/SAS** - Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
**Dyski twarde** - Zainstalowane 3 dyski SSD SATA o pojemności min. 1.92TB, 2,5“ Hot-Plug.
Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1.
Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
**Kontroler RAID** - Sprzętowy kontroler dyskowy, posiadający min. 4GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących.
**System operacyjny/System wirtualizacji -** Microsoft Windows Server 2022 Standard

Dodatkowo należy dostarczyć:

- nośnik CD/DVD umożliwiający downgrade do wersji Windows Server 2019 Standard
- 30x licencja Windows Server 2022/2019 User CALs

**Wbudowane porty** - 4 x USB z czego nie mniej niż 1x USB 3.0, 2xVGA z czego jeden na panelu przednim.
**Video** - Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
**Zasilacze** - Redundantne, Hot-Plug min. 800W każdy.
**Bezpieczeństwo:**

- Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.
  Możliwość wyłączenia w BIOS funkcji przycisku zasilania.
- BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła
- Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
- Moduł TPM 2.0
- Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera
- Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem

**Diagnostyka** - Możliwość wyposażony w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze.
**Karta Zarządzania** Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:

- zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
- zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
- szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;
- możliwość podmontowania zdalnych wirtualnych napędów;
- wirtualną konsolę z dostępem do myszy, klawiatury;
- wsparcie dla IPv6;
- wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;

- możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;
- możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;
- integracja z Active Directory;
- możliwość obsługi przez dwóch administratorów jednocześnie;
- wsparcie dla dynamic DNS;
- wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
- możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
- możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera

**Oprogramowanie do zarządzania** - Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:

- Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych
- integracja z Active Directory
- Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta
- Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish
- Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram
- Szczegółowy opis wykrytych systemów oraz ich komponentów
- Możliwość eksportu raportu do CSV, HTML, XLS, PDF
- Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.
- Grupowanie urządzeń w oparciu o kryteria użytkownika
- Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji
- Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach
- Szybki podgląd stanu środowiska
- Podsumowanie stanu dla każdego urządzenia
- Szczegółowy status urządzenia/elementu/komponentu
- Generowanie alertów przy zmianie stanu urządzenia.
- Filtry raportów umożliwiające podgląd najważniejszych zdarzeń
- Integracja z service desk producenta dostarczonej platformy sprzętowej
- Możliwość przejęcia zdalnego pulpitu
- Możliwość podmontowania wirtualnego napędu
- Kreator umożliwiający dostosowanie akcji dla wybranych alertów
- Możliwość importu plików MIB
- Przesyłanie alertów „as-is” do innych konsol firm trzecich
- Możliwość definiowania ról administratorów
- Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów
- Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)

- Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta
- Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
- Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.
- Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.
- Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile.
- Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.
- Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.
- Zdalne uruchamianie diagnostyki serwera.
- Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.
- Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.

**Certyfikaty** - Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001
Serwer musi posiadać deklaracja CE.
Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku. Wykonawca złoży dokument potwierdzający spełnianie wymogu.
Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.
**Dokumentacja użytkownika** - Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
**Warunki gwarancji** - 3 lata gwarancji producenta
Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.

Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.
Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy.
Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.
Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.
Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.
Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.
Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii.
Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.
Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
Możliwość rozszerzenia gwarancji przez producenta do 7 lat.
Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.
Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

## Część nr 2 urządzenie podtrzymujące napięcie – UPS – szt. 1;

Urządzenie zapewniające wydajną ochronę zasilania systemów i danych, a tym samym zapewniają niezawodną ochronę przed awariami zasilania, wahaniami prądu i zakłóceniami elektrycznymi.
**Wymagania ogólne:**
Moc wyjściowa (pozorna / czynna) - minimum 3000 VA, minimum 3000 W
Topologia - VI (line interactive)
Typ obudowy- Rack / Tower
Chłodzenie - Wymuszone, wewnętrzne wentylatory
Napięcie znamionowe (wartość skuteczna) - 230 V AC
Zakres napięcia wejściowego (wartości skuteczne) i tolerancja - 178 ÷ 281 V AC ± 2 %
Częstotliwość znamionowa napięcia wejściowego - 50 Hz
Zakres częstotliwości i tolerancja - 45 ÷ 55 Hz ± 1 Hz
Progi przełączania: sieć – UPS - 178 ÷ 281 V AC ± 2 %
Napięcie znamionowe (wartość skuteczna) - 230 V AC

Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca sieciowa - 195 ÷ 253 V AC ± 2 %
Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca rezerwowa - 230 V AC ± 5 %
Automatyczna regulacja napięcia (AVR) - ± 10 %
Kształt napięcia wyjściowego (przy pracy rezerwowej / sieciowej) - Sinusoidalny / Tak jak na wejściu
Częstotliwość znamionowa napięcia wyjściowego - 50 Hz
Filtracja napięcia wyjściowego - Filtr przeciwzakłóceniowy RFI/EMI, tłumik warystorowy
Progi przełączania: UPS – sieć - 183 ÷ 276 V AC ± 2 %
Czas przełączenia na pracę rezerwową - < 3 ms
Czas powrotu na pracę sieciową - 0 ms
Przeciążalność - > 105% - 15 s (wyłączenie UPS)
Akumulatory wewnętrzne - minimum 12 V / 7 Ah VRLA
Możliwość podpięcia modułów bateryjnych wymagane - minimum 1szt
Czas podtrzymania z baterii wewnętrznych ( 80 % / 50 % Pmax) - minimum 4 / 7 min
Maksymalny czas ładowania baterii wewnętrznych UPS do 90% pojemności baterii - po uprzednim rozładowaniu obciążeniem równym 80% Pmax (do wyłączenia się zasilacza) - do 4 h
Wymiary – Rack (wys. X szer. X gł.) - nie większe niż 132 x 440 x 630 mm
Masa zasilacza - nie większa niż 43 kg
Zabezpieczenie wejściowe - Przeciwzwarciowe – Bezpiecznik automatyczny 16 A / 250 V AC, Przeciwprzepięciowe.
Zabezpieczenie wyjściowe - Elektroniczne – przeciwzwarciowe i przeciążeniowe
Zabezpieczenia wejścia DC (akumulatory wewnętrzne) - Zabezpieczenie nadprądowe
Zabezpieczenia DC (zewnętrzny moduł bateryjny) - Zabezpieczenie nadprądowe
Przyłącza wyjściowe (liczba i typ gniazd) - minimum 9 gniazd z podtrzymaniem bateryjnym (w tym minimum 2 gniazda w standardzie PL z bolcem uziemiającym)
Sygnalizacja - Akustyczno – optyczna; graficzny wyświetlacz LCD
Interfejsy komunikacyjne - USB HID, SNMP/HTTP
Filtr teleinformatyczny (linii danych) – RJ45 - LAN 1 Gbit/s
Wsporniki do montażu w szafie RACK - wymagane
Oprogramowanie monitorująco-zarządzające - oprogramowanie w języku polskim do zarządzania i monitorowania pracy UPS, możliwość zdalnego włączenia / wyłączenia UPSa (poprzez SNMP), możliwość zdalnego wyłączenia zarządzanej sekcji gniazd, możliwość edycji nazw urządzeń na liście monitorowanych UPSów, wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów, wsparcie dla systemów Linux, Windows oraz wirtualizacji Hyper-V, Vmware, XenServer.
Możliwość ustawienie minimalnego stopnia naładowania akumulatorów, przy którym zasilacz uruchomi się po rozładowaniu akumulatorów i powrocie napięcia sieciowego - wymagane
Możliwość aktualizacji oprogramowania firmware przez użytkownika - wymagane
Deklaracje - CE
Normy - PN-EN 62040-1:2009, PN-EN 62040-2:2008
Gwarancja - min 36 miesięcy na elektronikę i 36 miesiące na akumulatory;
Serwis - autoryzowany serwis producenta zlokalizowany w Polsce, serwis realizowany w systemie door to door.
DODATKOWE OŚWIADCZENIA/DOKUMENTY - ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania - należy dołączyć do oferty dokument potwierdzający spełnienie wymagań, jeżeli oferowana jest niestandardowa, rozszerzona gwarancja to wymagane jest by realizowana była wyłącznie przez serwis producenta - należy przedstawić odpowiednie oświadczenie

producenta, oświadczenie producenta o spełnieniu minimalnych wymaganych parametrów specyfikacji, karta katalogowa oferowanego sprzętu.

## Część nr 3 router –switche – szt. 1

**Porty przełącznika**: minimum 52x 10/100/1000Base-T RJ45 oraz minimum 4x 1/10GBase-X SFP+
**Port konsolowy:** RJ45 (RS-232)
**Port USB:** minimum 1 port co najmniej w standardzie 2.0
**Szybkość przełączania:** minimum 176Gb/s
**Przepustowość:** minimum 130Mp/s (dla pakietów 64Kb)
**Bufor pakietów:** minimum 1,5 MB
**Ramki Jumbo:** minimum 10k
**Tablica adresów MAC:** minimum 16k
**Adresy MAC – Multicast:** minimum 1k
**Tablica ACL:** minimum 512
**Tablica VLAN:** minimum 4094
**Taktowanie procesora:** minimum 800MHz
**Pamięć Flash:** minimum 32MB
**Pamięć RAM:** minimum 256MB
**Temperatura pracy:** zakres minimum 0°C - 50°C
**Wilgotność względna:** zakres minimum 10% - 90% (bez kondensacji)
**Zasilanie:** zabudowany zasilacz 230V AC
**Pobór mocy:** maksymalnie 50W
**Zabezpieczenie przeciwprzepięciowe:** minimum 6kV
**Wymiary:** maksymalna: szerokość 440 mm, wysokość 44mm , głębokość 280mm
**Certyfikaty bezpieczeństwa**: CE, RoHS

**Algorytm:** Store and Forward
**VLAN:** Voice VLAN, Port based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN, VLAN Translation, N:1 VLAN Translation, GVRP, IEEE 802.1Q, Normal QinQ, Flexible QinQ
**DHCP:** IPv4/IPv6 DHCP Client,IPv4/IPv6 DHCP Relay, Option 82, IPv4/IPv6 DHCP Snooping,IPv4/IPv6 DHCP Server
**Spanning tree:** IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Multi-Process MSTP, Root Guard, BPDU guard, BPDU forwarding
**Protekcja ringowa:** ITU-T G.8032 – recovery time < 50ms, Fast Link, Loopback Detection
**Agregacja łączy:** IEEE 802.3ad (LACP), 64 groups per device / 8 ports per group, load balance
**Bezpieczeństwo:** Storm Control based on packets, Port Security, MAC Limit based on VLAN and Port, Anti-ARP-Spoofing , Anti-ARP-Scan, ARP Binding, Gratuitous ARP, ARP Limit, Anti ARP/NDP Cheat, Anti ARP Scan, ND Snooping, DAI, IEEE 802.1x, Authentication, Authorization, Accounting, Radius IPv4/IPv6, TACACS+, MAB, Port and MAC based authentication, Accounting based on time length and traffic, Guest VLAN and auto VLAN,
**Multicast:** IGMP v1/v2/v3 snooping and L2 Query, IGMP Fast leave, MVR, MLD v1/v2 Snooping, IPv4/IPv6 DCSCM, IGMP authentication
**QoS:** 8 queques per port, Bandwidth Control, Flow Control: HOL, IEEE802.3x, Flow Redirect, Classification based on ACL, COS, TOS, DiffServ, DSCP, port number; Traffic Policing, PRI

Mark/Remark, IEEE 802.1p, Queuing Method: Strict Priority, Weighted Deficit Round Robin, Strict priority in Weighted Deficit Round Robin; DNS Client, DNS Relay
**Lista kontroli dostępu:** IP Src/Dst ACL, MAC Src/Dst ACL, MAC-IP ACL, User-Defined ACL, Time Range ACL, port number TCP/UDP ACL, VLAN ACL, REDIRECT and Statistics based on ACL, Precedence, Vlan Tag/Untag, Rules can be configured to port and VLAN
**Diagnostyka:** sFlow, Traffic Analysis, RSPAN, VCT, Ping, Trace Route, Dying GASP
**Zarządzanie:** TFTP/FTP, CLI, Telnet, Console, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), SNMP v1/v2c/v3, SNMP Trap, Public & Private MIB interface, RMON 1,2,3,9, Syslog (IPv4/IPv6), SNTP/NTP (IPv4/IPv6), Dual IMG, Multiple Configuration Files, Port Mirror, IEEE 802.3ah/802.1ag OAM, ULDP (like UDLD), LLDP/LLDP MED., VSF (4 devices in one stack) – hardware stacking
**Oprogramowanie oraz wsparcie techniczne:** oprogramowanie przełącznika (firmware) dostępne bez ograniczeń czasowych, przez cały okres cyklu życia urządzenia, poprzez Internet, wsparcie techniczne dystrybutora bez konieczności wykupu dodatkowych usług
**Gwarancja:** lifetime + min. 1 rok po wycofaniu produktu z linii produkcyjnej. W przypadku gdy produkt zostanie wycofany wcześniej niż 5 lat od daty zakupu, gwarancja powinna obowiązywać min. 6 lat.

## Część nr 4 zakup szafy serwerowej szt. 1 z patch panel rack – szt. 2

Typ - Szafa serwerowa 19” z kółkami skrętnymi
Wymiar - 27U, szerokość: 600mm, głębokość: 1000mm
Drzwi przednie - Stalowe, perforowane, zamykane na klucz
Drzwi tylnie - Stalowe, perforowane, zamykane na klucz
Osłony boczne - Stalowe, demontowalne, zamykane na klucz
Istotne elementy konstrukcyjne - 4 belki rackowe
Przepusty kablowe (umieszczone z góry i z dołu szafy)
Panel wentylacyjny
Typ: dachowy
Ilość wentylatorów: 4
Termostat
Wyposażenie:
2x Patch panel UTP 19” 1U 48-porty kat. 6 złącza LSA, z polami opisowymi
4x Organizator kabli 19” 1U
1x listwa zasilająca 19” 1U min 8 x 230V
1x tacka 19” 1U
Warunki gwarancji
Min. 1 rok gwarancji producenta

## Część nr 5 urządzenie brzegowe UTM – szt. 1

Dostarczone urządzenie musi posiadać:

**PARAMETRY SPRZĘTOWE**
1. Urządzenie musi być wyposażone w co najmniej:
    a. 8 wbudowanych interfejsów 10/100/1000 Ethernet (RJ45)

b. jeden port konsoli szeregowej RJ45,
c. jeden dedykowany port zarządzający 10/100/1000.

2. Urządzenie musi być wyposażone w niemechaniczny zasób dyskowy o pojemności co najmniej 120 GB na potrzeby systemu operacyjnego i logów.
3. Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe:
a. co najmniej 2.0 Gbps dla rozpoznawania i kontroli aplikacji,
b. co najmniej 0.9 Gbps dla rozpoznawania kontroli aplikacji przy włączonych funkcjach bezpieczeństwa: IPS, antywirus, antyspyware, blokowanie typów plików, z włączonym logowaniem na niemechaniczne zasoby dyskowe urządzenia,
c. co najmniej 1.5 Gbps dla IPSec VPN,
d. co najmniej 36 000 nowych sesji na sekundę.
e. co najmniej 190 000 równoległych sesji.

4. Urządzenie musi obsługiwać nie mniej niż 3 wirtualne routery posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Zamawiający dopuszcza rozwiązania, gdzie system urządzenia wymaga, aby tablica routingu była powiązana z wirtualnym systemem w relacji 1:1 wówczas należy przewidzieć w ofercie trzykrotnie większą liczbę wirtualnych firewalli obsługiwanych przez urządzenie aniżeli wymagana w pozostałych wymaganiach dla urządzenia.
5. Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 1900 reguł polityk bezpieczeństwa.
6. Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 2900 reguł polityk translacji adresów.

**WYMAGANIA OGÓLNE**
7. Musi to być specjalizowane urządzenie sieciowe (tzw. appliance) mogące pracować jako pojedyncze urządzenie oraz jako klaster wysokiej dostępności (HA) w trybach Active/Standby, Active/Active.
8. Całość sprzętu i oprogramowania musi być dostarczona i wspierana przez jednego producenta. Producent oferowanego rozwiązania musi być obecny w rynkowych raportach Gartner Magic Quadrant for Enterprise Network Firewalls w części (ćwiartce) Leaders przynajmniej od 2 lat.
9. Urządzenia muszą umożliwiać działanie w następujących trybach pracy:
a. rutera (tzn. w warstwie 3 modelu OSI),
b. mostu (tzn. w warstwie 2 modelu OSI),
c. w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych; Musi pracować w trybie przezroczystego łączenia interfejsów w pary.).
d. w trybie pasywnego nasłuchu (sniffer/tap).
10. System musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu.
11. Urządzenia firewall muszą posiadać separację logiczną zasobów służących do przetwarzania ruchu od zasobów służących do zarządzania urządzeniem.
12. Urządzenie musi posiadać dedykowane zasoby/rdzenie procesora/procesorów do funkcji zarządzania urządzeniem lub możliwość ustawienia dedykowanych zasobów/rdzeni procesora/procesorów do funkcji zarządzania urządzeniem.
13. Urządzenia firewall muszą wspierać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Pod-interfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4000 znaczników VLAN.

14. Urządzenia firewall muszą wspierać protokół LACP.
15. Urządzenia firewall muszą zgodnie z ustaloną polityką prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
16. Urządzenia firewall muszą działać zgodnie z zasadą bezpieczeństwa najmniejszego możliwego przywileju. Musi blokować wszystkie aplikacje i ruch sieciowy, poza tymi które w regułach polityki bezpieczeństwa skonfigurowanych na firewall są wskazane jako dozwolone.
17. Polityka zabezpieczeń firewall musi uwzględniać
    a. adresy IP źródłowe i docelowe,
    b. protokoły i usługi sieciowe,
    c. aplikacje,
    d. kategorie URL,
    e. użytkowników aplikacji i grupy,
    f. reakcje zabezpieczeń,
    g. logowanie zdarzeń (początek i koniec sesji),
    h. strefa wejściowa i wyjściowa

18. Urządzenie musi umożliwiać rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów, na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65535 dostępnych portach. Przy tym wydajność kontroli firewalla stanowego i kontroli aplikacji całego ruchu nie może być mniejsza, niż wskazano w wymaganiach wydajnościowych urządzeń.
Urządzenie musi wykrywać co najmniej 3700 predefiniowanych aplikacji wspieranych przez producenta (takich jak DNS over HTTPS, Telegram, Skype, Tor, BitTorrent, MQTT, Modbus, DNP3, Siemens S7) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi.
19. Urządzenia firewall muszą pozwalać na blokowanie transmisji plików, nie mniej niż: .pif, .scr, .cpl, .dll, .ocx, .exe, .class, .jar, vbe, .hta, .wsf, .torrent, .7z, .rar, .bat, .cab, .msi, .lnk, szyfrowany MS Office, szyfrowany RAR, szyfrowany ZIP. Rozpoznawanie pliku musi odbywać się na podstawie zawartości i metadanych pliku.
20. Urządzenia firewall muszą zarządzane z linii poleceń (CLI) oraz graficznej konsoli Web GUI. Nie jest dopuszczalne, aby istniała konieczność instalacji dedykowanego oprogramowania/klienta na stacji administratorów w celu zarządzania systemem.
21. Urządzenia firewall muszą być wyposażone w interfejs API będący integralną częścią systemu zabezpieczeń, za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI). Jeżeli dostęp do API, jego dokumentacji, zadawania pytań pomocy wymaga licencji lub subskrypcji – należy dostarczyć odpowiednie dla minimum 30 administratorów.
22. Dostęp do urządzeń i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.
23. Urządzenia firewall muszą umożliwiać uwierzytelnianie administratorów za pomocą nie mniej niż:

a. baza lokalna,
b. serwer Radius,
c. serwer TACACS+,
d. serwer AD/LDAP.

Dla dostępu administracyjnego SSH musi być wspierane uwierzytelnianie za pomocą kluczy SSH a dla dostępu GUI za pomocą certyfikatów kryptograficznych.

24. Urządzenia firewall muszą zapewniać możliwość automatycznego i transparentnego ustalenia tożsamości użytkowników sieci i integrować się w tym zakresie z systemami:
a. Active Directory,
b. Terminal Services.

25. Polityka kontroli dostępu (urządzeń firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym mających wspólny adres IP źródłowy, ustalanie tożsamości musi odbywać się również transparentnie.

26. Urządzenia firewall muszą pozwalać na lokalne zbieranie (na dysk urządzenia) i analizowanie logów, korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach, filtrowaniu url, deszyfracji SSL.

27. Urządzenie musi dostarczać predefiniowane przez producenta raporty standardowe jak i możliwość tworzenia raportów niestandardowych. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu.

28. Urządzenie musi pozwalać na zapisanie raportów na urządzeniu i uruchamiania w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.

29. Urządzenia firewall muszą umożliwiać tworzenie dynamicznych grup użytkowników. Przynależność do grupy musi bazować na etykietach a proces oznaczania etykiet musi pozwalać na użycie:
a. reakcji na zdarzenie/log (np. wystąpienie zagrożenia)
b. API

30. Urządzenia firewall muszą posiadać funkcję dynamicznego pobierania i odświeżania informacji o zasobach VM i ich adresach IP i etykietach (tagi) dla środowiska VMWare ESX i VMWare vCenter. Tak pobierane adresy IP muszą pozwalać na budowanie dynamicznych obiektów, które można potem wykorzystywać w polityce bezpieczeństwa urządzeń.

31. Urządzenia firewall muszą obsługiwać protokoły routingu dynamicznego, minimum: BGP i OSPF.

32. Urządzenia firewall muszą obsługiwać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.

33. Urządzenia firewall muszą posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.

34. Wykonywanie operacji translacji adresów NAT musi być odnotowywane w logach ruchu sieciowego za pomocą dedykowanego pola lub flagi oraz odpowiednich kolumn ze szczegółami NAT.

35. Urządzenia firewall muszą pozwalać na selektywne wysyłanie logów w zależności od ich rodzaju.

36. Urządzenia firewall muszą obsługiwać możliwość deszyfrowania ruchu użytkowników w celu inspekcji dla protokołów HTTP/2, SSL, TLS 1.2, TLS 1.3.

37. Urządzenia firewall muszą posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i inspekcji rozdzielny od polityk bezpieczeństwa.

38. Wykonywanie operacji deszyfrowanie ruchu musi być odnotowywane w logach urządzeń w dedykowanej do tego celu sekcji. Musi zawierać informacje ułatwiające diagnostykę m.in. informacje o błędach, typ i rozmiar klucza, wersja TLS. Musi istnieć mechanizm automatycznego wykluczania z szyfrowania problematycznych stron na bazie tego logu.
39. Wykonywanie operacji deszyfrowania ruchu musi umożliwiać wykorzystanie mechanizmów filtrowania URL.
40. Dla deszyfrowania ruchu TLS 1.3 wymagane jest wsparcie dla X25519, X448 oraz minimum dla zestawów protokołów: TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384 oraz TLS_CHACHA20_POLY1305_SHA256.
41. Urządzenia firewall muszą posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
42. Urządzenia firewall muszą wspierać zarządzanie pasmem (QoS) i ustawiania dla aplikacji priorytetu oraz pasma.
43. Urządzenia firewall muszą umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia trasowania (tzw. routing-based VPN).
44. Dla IKE wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
45. Dla IPsec wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
46. Urządzenia firewall muszą zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tuneli SSH.
47. Wsparcie serwisowe (techniczne) i gwarancja dla systemu (zwana dalej wsparciem) będzie świadczone przez producenta lub autoryzowane przez producenta centrum serwisowe, niezależne od Wykonawcy, realizowane we współpracy z producentem, przez okres 12 miesięcy od daty odbioru sprzętu.

**WYMAGANIA FUNKCJI BEZPIECZEŃSTWA**

48. Urządzenia firewall muszą posiadać funkcję wykrywania i blokowania ataków/intruzów w warstwie 7 modelu OSI (nazywany często również jako IPS). Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
49. Bezpośrednio w GUI urządzenia musi istnieć możliwość uruchomienia/aktywowania nowej aktualizacji sygnatur albo powrotu do starszej wersji sygnatur, gdyby taka potrzeba zachodziła.
50. Urządzenia firewall muszą posiadać funkcję ręcznego tworzenia sygnatur (IPS) bezpośrednio na urządzeniu.
51. Urządzenia firewall muszą posiadać funkcję inspekcji antywirusowej uruchamianą per aplikacja/polityka oraz wybrany protokół minimum: http, http2, smtp, imap, pop3, ftp, smb. Baza sygnatur anty-wirus musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż raz na 48 godzin i pochodzić od tego samego producenta co firewall.
52. Urządzenia firewall muszą posiadać funkcję anty-spyware. Baza sygnatur musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co systemu firewall.
53. Urządzenie musi posiadać funkcję filtrowania URL.

54. Urządzenie musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (a nie tylko filtrującego) ruch w politykach bezpieczeństwa.

55. Funkcja filtrowania URL musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.

56. Wymagane jest posiadanie oddzielnych kategorii URL dla zagrożeń typu malware, phishing, C2C, ransomware oraz ostatnio zarejestrowane domeny.

57. Urządzenie musi zapewniać ochronę przed atakami typu „Drive-by-download" poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj" dla funkcji blokowania kategorii URL.

58. Urządzenia firewall muszą umożliwiać przechwytywanie i przesyłanie do zewnętrznych systemów typu „SandBox" plików wykonywalnych PE i DLL przechodzących przez firewall. Systemy sandbox, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików, adresów IP, DNS i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik. Maksymalny interwał aktualizacji sygnatur 48 godzin.

59. Urządzenia firewall muszą realizować ochronę DNS w zakresie:

a. wykrywania zapytań do domen złośliwych (baza domen musi mieć co najmniej 10 milionów wpisów),

b. możliwości skonfigurowania fałszowania odpowiedzi na zapytania DNS zaklasyfikowane jako niebezpieczne (tzw. DNS sinkholing),

c. wykrywania domen generowanych dynamicznie przez złośliwe oprogramowanie w celu uniknięcia wykrycia kanałów komunikacyjnych (tzw. domeny DGA),

d. wykrywanie domen dynamicznych Dynamic DNS,

e. wykrywania nadużyć protokołu DNS w celu infiltracji i eksfiltracji danych.

## Część nr 6 oprogramowanie licencyjne do UTM – szt. 1

W przypadku gdy jakakolwiek funkcjonalność UTM lub parametr ilościowy wymagają licencji, Zamawiający wymaga ich dostarczenia w celu zapewnienia pełni wymaganych właściwości przez okres 12 miesięcy od daty odbioru sprzętu.

## Część nr 7 urządzenie do robienia backupuów NAS wraz z 4 dyskami 12TB – szt. 1

Procesor - Intel® Celeron® N5105/N5095 4-core/4-thread processor, burst up to 2.9 GHz
Obudowa - Rack 2U o wymiarach, 88,6 × 482,14 × 346,43 mm
(wys. x szer. x gł.) wraz z szynami umożliwiającymi montaż w szafie rack
Pamięć RAM - 4 GB SO-DIMM DDR4 (1 x 4 GB)
Ilość obsługiwanych dysków - 8 dysków 3,5-calowych SATA 6 Gb/s, 3 Gb/s
Dyski - 4 dyski 3,5-cala HDD, min. 12TB SATA, 7200RPM, 256MB cache, min. 2,5 mln MTBF, przeznaczony do pracy 24/7, serii Enterprise, gwarancja producenta 60 miesięcy
Interfejsy sieciowe -2 porty 2,5 Gigabit sieci Ethernet (2,5G/1G/100M)
obsługa VLAN i Jumbo Frame.

Porty - 2x USB 2.0, 2x USB 3.2 Gen 2, 1x HDMI 1.4b
Wskaźniki LED - HDD 1–8, stan, LAN, rozszerzenie, zasilanie
Obsługa RAID - Pojedynczy dysk, JBOD, RAID 0,1,5,5+Spare,6,6+Spare,10 i 10+Spare, RAID50, RAID60. Obsługa BITMAP w celu przyspieszenia odbudowy. Możliwość skonfigurowania Global Spare Disk.
Funkcje RAID - Możliwość zwiększania pojemności i migracja między poziomami RAID online.
Szyfrowanie - Możliwość szyfrowania całych woluminów kluczem AES 256 bitów.
System Operacyjny - Apple Mac OS 10.10 or later
Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 or later Linux
IBM AIX 7, Solaris 10 or later UNIX
Microsoft Windows 7, 8, and 10
Microsoft Windows Server 2008 R2, 2012, 2012 R2 and 2016, 2019
Stacja monitoringu - Obsługa do 24 kamer IP (8 licencji domyślnie).
Protokoły - CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
Usługi - Stacja monitoringu, Windows ACL, Integracja w Windows ADS, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Obsługa paczek QPKG, Funkcja Virtual Disk umożliwiająca zwiększenie pojemności serwera przy pomocy protokołu iSCSI, Montowanie obrazów ISO, Replikacja w czasie rzeczywistym, Serwer RADIUS, Klient LDAP, Serwer Syslog, Virtualization Station
Zarządzanie dyskami - SMART, sprawdzanie złych sektorów
Język GUI - Polski
Gwarancja i serwis - 36 miesięcy, producenta
Pobór mocy:
Uśpienie: 31.742 W
Praca: 55.83 W
System plików - Dyski wewnętrzne EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+
Liczba kont użytkowników - 4096
Liczba grup - 512
Liczba udziałów - 512
Max ilość połączeń (CIFS) - 1500
Max liczba migawek - 1024
Zasilanie - 300 W, 100–240 V
Wentylator - 80mm, 12VDC
UPS - Obsługa sieciowych awaryjnych zasilaczy UPS.

## Część nr 8 oprogramowanie do robienia backup (kopii zapasowych) – szt. 1

Wymagania 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 dostępnej z poziomu przeglądarki internetowej,
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 z poziomu jednej konsoli,
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 bezpośrednio 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.
System pozwala na zautomatyzowaną replikację danych.

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: 6.7+.
-Dowolne inne w sposób agentowy

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 gniazd na procesor na fizycznych hostach maszyn wirtualnych lub ilości maszyn wirtualnych,
-Ilości repozytoriów - dla GIT,
-ilości użytkowników dla ekosystemu Microsoft Office 365.

Licencje umożliwiają :
-wieczyste zabezpieczenie endpointów fizycznych,
-wieczyste zabezpieczenie serwerów fizycznych,

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,

Obowiązuje przez okres minimum 36 miesięcy.

Wdrożenie:

Wdrożenie musi zostać przeprowadzone bezpośrednio przez producenta oprogramowania,
Wdrożenie musi się odbyć w języku polskim,
Wdrożenie musi obejmować krótkie, podstawowe szkolenie z obsługi oprogramowania.

## Część nr 9 stacje robocze – szt.4

**Komputery stacjonarne wraz z monitorami, klawiaturami orasz myszami o minimalnych wymaganiach technicznych komputerów:**

Typ - Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta
Zastosowanie - Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna
Procesor - Procesor wielordzeniowy ze zintegrowaną grafiką, osiągający w teście PassMark CPU Mark wynik min. 13 800 punktów na dzień 6.06.2023
Pamięć RAM - 8 GB DDR4 3200 MHz non-ECC możliwość rozbudowy do min 64GB, min. 1 slot wolny
Pamięć masowa - SSD 256GB M.2 NVMe PCIe

Napęd optyczny - Nagrywarka DVD +/-RW o prędkości min. 8x
Grafika - Zintegrowana karta graficzna
Wyposażenie multimedialne - Karta dźwiękowa zintegrowana z płytą główną, port audio combo (słuchawki + mikrofon )na panelu przednim, na tylnym audio out
Obudowa - Typu SFF z obsługą kart rozszerzeń o niskim profilu, napęd optyczny w dedykowanej wnęce zewnętrznej slim. Suma wymiarów mierzona po krawędziach obudowy nie może przekraczać 678 mm, waga max 6kg,
Zasilacz o mocy max. 180W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 81% przy obciążeniu zasilacza na poziomie 100%,
Wbudowany w zasilaczu system diagnostyczny do sprawdzenia zasilacza bez konieczności włączania komputera, zasilacz w oferowanym komputerze musi się znajdować na stronie http://www.plugloadsolutions.com/80pluspowersupplies.aspx, do oferty należy dołączyć wydruk potwierdzający spełnienie wymogu 80plus, w przypadku, kiedy u producenta występuje kilka zasilaczy, które są montowane na etapie produkcji w fabryce załączyć wydruki dla wszystkich zasilaczy.
Wydruki 80plus musza być potwierdzone przez producenta lub dołączone oświadczenie producenta komputera iż wskazane zasilacze przez wykonawcę spełniają 80plus.
Obudowa musi posiadać wbudowany wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED np. przycisku POWER [ tzn. barw i miganie ] W szczególności musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię procesora.
Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wnęk zewnętrznych oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego.
Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS.
Zgodność z systemem operacyjnym - Potwierdzenie kompatybilności komputera na daną platformę systemową (wydruk ze strony)
Bezpieczeństwo - Ukryty w laminacie płyty 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. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej.
System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. Działający w pełni, bez okrojonych funkcjonalności nawet w przypadku uszkodzonego dysku, braku dysku lub sformatowanym dysku, dostępu do sieci i internetu oraz bez konieczności podłączenia urządzeń wewnętrznych i zewnętrznych oraz bez konieczności pobierania i instalowania np. na ukrytej pamięci flash BIOS
BIOS - BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, nazwę producenta komputera, model komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy.
Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych oraz dodatkowego oprogramowania typu system diagnostyczny odczytania z wewnętrznego menu BIOS informacji o: wersji BIOS, nr seryjnym komputera, dacie wyprodukowania komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci

z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, obecnej, minimalnej i maksymalnej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, MAC adresie zintegrowanej karty sieciowej,
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 ustawienia hasła systemowego/użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) oraz uprawniającego do samodzielnej zmiany tego hasła przez użytkownika (bez możliwości zmiany innych parametrów konfiguracji BIOS) przy jednoczesnym zdefiniowanym haśle administratora.
Możliwość wyłączania portów USB w tym:
- tylko portów USB znajdujących się na przednim panelu obudowy,
- tylko portów USB znajdujących się na tylnym panelu obudowy.
- wszystkich portów USB
- pojedynczo
Warunki gwarancji - 3-letnia gwarancja producenta świadczona na miejscu u klienta, Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty.
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 – do oferty należy dołączyć link strony.
System Operacyjny - Zainstalowany system operacyjny Windows 11 Professional, klucz licencyjny musi być zapisany trwale w BIOS.
Porty I/O - Wbudowane porty:
- panel przedni : 2x USB 3.2 gen 1, 2x USB 2.0, 1x audio (dopuszcza się combo),
- panel tylny: 1x audio out, 2x USB 3.2 gen 1, 2x USB 2.0, 1x DP 1.4, 1x HDMI 1.4b, 1x RJ45
Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki dedykowana dla danego urządzenia; wyposażona w : 1x PCI Express x16, 1x PCI Express x1, min. 2 złącza DIMM z obsługą do 64GB DDR4 pamięci RAM, min. 2 złącza SATA w tym 1 szt SATA 3.0, 1 złącze M.2 dla dysków SSD, 1 złącze M.2 dla bezprzewodowej karty WiFI
Wymagania dodatkowe - Klawiatura USB w układzie polski programisty
Mysz USB z klawiszami oraz rolką (scroll)
Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu.
Dodatkowe oprogramowanie - Dołączone do oferowanego komputera oprogramowanie z nieograniczoną licencją czasowo na użytkowanie umożliwiające :
- upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,
- możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji :

a. o poprawkach i usprawnieniach dotyczących aktualizacji

b. dacie wydania ostatniej aktualizacji
c. priorytecie aktualizacji
d. zgodność z systemami operacyjnymi
e. jakiego komponentu sprzętu dotyczy aktualizacja
f. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e.

- wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne
- możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga.
- rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty ( dd-mm-rrrr )
- sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą ( dd-mm-rrrr ) i wersją ( rewizja wydania )
- dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml
- raport uwzględniający informacje o : sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą ( dd-mm-rrrr ) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.

Wymagane minimalne parametry techniczne monitora:
Typ ekranu Ekran ciekłokrystaliczny z aktywną matrycą min. 21,45" (16:9)
Rozstaw pikseli 0,249x0,241mm
Jasność 250 cd/m2
Kontrast Typowy 3000:1
Czas reakcji matrycy max 5ms (Gray to Gray)
Rozdzielczość maksymalna 1920 x 1080 przy 60Hz
Color Gamut 72% (CIE 1931)
Zużycie energii Normalne działanie 14,1 W (typowe), 22W (maksymalne), tryb wyłączenia aktywności mniej niż 0,3W
Powłoka powierzchni ekranu Antyodblaskowa utwardzona
Podświetlenie System podświetlenia LED
Bezpieczeństwo Monitor musi być wyposażony w tzw. Kensington Slot - gniazdo zabezpieczenia przed kradzieżą.
Wbudowane w monitor narzędzie diagnostyczne umożliwiające zdiagnozowanie problemu wyświetlania obrazu na ekranie (kwestia karty graficznej czy monitora)
Waga bez podstawy Maksymalnie 2,5 kg
Waga z podstawą + kable Maksymalnie 3 kg
Wymiary bez podstawy Wysokość : max. 332 mm
Szerokość : max. 553 mm
Głębokość : max. 50 mm
Wymiary z podstawą Wysokość : max. 421 mm
Szerokość : max. 553 mm
Głębokość : max. 179 mm
Zakres regulacji Tilt Wymagany, od -5 do +21 lub min. regulacja 26 stopni
Kolor obudowy czarny

Złącze 1x 15-stykowe złącze D-Sub, 1 x HDMI 1.4
Gwarancja 3 lata na miejscu u klienta
Czas reakcji serwisu - do końca następnego dnia roboczego
Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta– dokumenty potwierdzające załączyć do oferty.

## Część nr 10 szkolenie pracowników – pod kątem korzystania z wdrożonych systemów informatycznych

Wykonawca obowiązuje się przeszkolić obsługę informatyczną Zamawiającego z zakresu zarządzania urządzeniami, programami zainstalowanymi, ich konfiguracją oraz administrowania siecią. Wykonawca zobowiązuje się do zorganizowania szkolenia 4 dni x 8 h (łącznie 32 h)

## WYMAGANIA DO CAŁEGO ZAMÓWIENIA:

Ad. 1-9 Wszystkie powyższe dostawy powinny zawierać cenę usług informatycznych w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania.
Wymagania zawarte w szczegółowym opisie przedmiotu zamówienia są minimalnymi. Wykazanie, że proponowany produkt posiada lepsze parametry ciąży na Wykonawcy składającym ofertę.

**Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania.**
Zamawiający wymaga, aby wszystkie dostarczone urządzenia zostały umieszczone (zamontowane) i uruchomione we wskazanych przez Zamawiającego miejscach przeznaczenia, w uzgodnionym przez obie strony terminie. Sposób montażu sprzętu ma być dostosowany do technologii wykonania oraz ma być przeprowadzony zgonie z zaleceniami producenta.

**Warunki serwisu technicznego**
Wsparcie techniczne musi być świadczone w języku polskim przez producenta lub oficjalnego partnera producenta urządzeń w zakresie świadczenia pomocy serwisowej.

Wraz z dostarczonym sprzętem będzie świadczony dostęp do strony pomocy technicznej producenta oraz możliwość pobierania aktualizacji oprogramowania związanego z oferowanym sprzętem.