**Załącznik nr 1 do SWZ**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**„Rozwój cyfryzacji i cyberbezpieczeństwa Starostwa Powiatowego   
we Włocławku”**

Przedmiotem zamówienia jest zakup wraz z dostawą oprogramowania oraz fabrycznie nowego sprzętu informatycznego wraz z montażem, instalacją, konfiguracją i uruchomieniem, w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa współfinansowanego ze środków Europejskiego Funduszu Rozwoju Cyfrowego - Umowa o powierzenie grantu o numerze FERC.02.02-CS.01 001/23/0948/FERC.02.02-CS.01-001/23/2024. Niniejsze zamówienie obejmuje:

1. **Zarządzalny przełącznik sieciowy – Typ-1 (2 szt.),**
2. **Zarządzalny przełącznik sieciowy – Typ 2 (10 szt.),**
3. **Serwery backupu (2 szt.),**
4. **Macierz dyskowa (1 szt.),**
5. **Urządzenie do deduplikacji i zabezpieczenia danych (2 szt.),**
6. **Oprogramowanie do zarządzania klastrem i systemem bazodanowym (wykonywania kopii zapasowych) (1 sztuka),**
7. **Zasilacz do serwerów (UPS) Typ 1 (2 szt.),**
8. **Zasilacz do stacji końcowych Typ 2 (15 szt.).**
9. **Zarządzalny przełącznik sieciowy Typ 1. – 2 szt.**

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

* Ilość portów 12 portów SFP+ oraz 12 portów 1/2,5/5/10G niezależne
* Chłodzenie od przodu do tyłu obudowy
* Tablica MAC min. 16K
* Tablica 4K ARP/ 512 NDP
* Bufor 32Mb
* MTBF min. 779640 godzin
* Wydajność min. 357 Mp/s
* Przepustowość min. 480 Gb/s
* Port USB-C
* 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
* Interfejs web umożliwiający automatyczne przypisanie konfiguracji do portów właściwej dla protokołów czy też producenta: NVX, AMX, NDI, ZeeVee, Aurora, Kramer, LibAV, Dante Video, SDVoE, AES67, Q-SYS, Audio Dante, AVB, Crestron DigitalMedia AV, NUCLEUS Converged AV, Shure, Sonos, Visionary AV
* Wymaga się aby powyższe szablony konfiguracji były stworzone przez producenta przełącznika a interfejs web w sposób jednoznaczny wskazywał że dany producent AV czy protokół jest obsługiwany przez dany szablon.
* Wymaga się aby producent dostarczył kontroler w formie aplikacji umożlwiający przypisanie profilu AV do grupy przełączników w sposób automatyczny
* Wymaga się aby interfejs web miał możliwość wykonywania poleceń tekstowych CLI bez potrzeby tworzenia oddzielnego połączenia Telnet lub SSH.
* IPv4/IPv6 Multicast filtering
* IGMPv3 MLDv2 Snooping
* ASM & SSM
* IGMPv1,v2 Querier
* Policy-based routing (PBR)
* LLDP-MED
* Spanning Tree
* Green Ethernet
* STP
* MTP
* RSTP
* EEE (802.3az)
* GVRP/GMRP
* Q in Q,
* Private VLAN
* DOT1X
* MAB
* Captive Portal
* DHCP Snooping
* Dynamic ARP
* Inspection
* IP Source Guard
* CPU min ARMv8 1.8Ghz
* Min 2GB RAM
* Min 512MB 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
* Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh
* 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

Wymaga się aby urządzenie posiadało deklarację zgodności CE.

Gwarancja:

Wymaga się aby urządzenie było objęte gwarancją producenta na okres min. 24 miesiące, 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 serwis w okresie gwarancji.

1. **Zarządzalny przełącznik sieciowy Typ 2. – 10 szt.**

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. 16000
* Tablica ARP/NDP min. 850
* 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 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 4000
* OSPFv3 min. sąsiadów na interfejs 100
* UDLD
* LLPF
* DHCPv6 Snooping
* wysyłanie alertów na email
* MMRP
* Ilość ACL min. 100
* Ilość reguł na listę min. 1000 na wejściu i 500 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

Wymaga się aby urządzenie posiadało deklarację zgodności CE.

Gwarancja:

Wymaga się aby urządzenie było objęte gwarancją producenta na okres min. 24 miesiące, 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 serwis w okresie gwarancji.

Wymagania w zakresie instalacji i wdrożenia zarządzanych przełączników sieciowych Typ1 oraz Typ 2:

Zamawiający wymaga:

1. Instalacji dostarczonych przełączników we wskazanych przez Zamawiającego punktach dystrybucji okablowania
2. Wykonawca musi zapewnić również kompatybilne wkładki światłowodowe SFP+ 10GB WDM do zestawienia połączenia wszystkich przełączników typu 2 do przełącznika typu 1 (zamawiający posiada rozprowadzoną sieć światłowodową w urzędzie. Maksymalna odległość między przełącznikami wynosi 2km)
3. Konfiguracji funkcjonalności warstwy II: VLAN, Spanning Tree, agregacji łączy.
4. Konfiguracji zarządzania (SSH, HTTPS, SNMP).
5. Konfiguracji logowania zdarzeń.

**3. Serwer backupu - 2 szt.**

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | * Obudowa Rack o wysokości max 1U * Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, pozwalający jednoznacznie stwierdzić, czy system działa poprawnie i pokazujący podstawowe stany działania serweraw tym adres IP karty zarządzającej * 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. * Obsługa procesorów 32 rdzeniowych. * Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. * Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. * Płyta główna powinna obsługiwać do 1TB pamięci RAM. |
| **Chipset** | * Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. |
| **Procesor** | * Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.9GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 176 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. |
| **RAM** | * 4x 64GB DDR5 RDIMM 5600MT/s, |
| **Dyski twarde** | * Zainstalowane dwa dyski M.2 NVMe SSD o pojemności min. 480GB z możliwością konfiguracji RAID 1. |
| **Gniazda PCI** | * Dwa sloty PCIe LP |
| **Interfejsy sieciowe/FC/SAS** | * Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) * Czteroportowa karta sieciowa 10Gb Ethernet w standardzie BaseT * 4x kabel DAC 10GbE SFP+/SFP+ min. 5m * Czteroportowa karta 12Gb SAS HBA |
| **Wbudowane porty** | * 4 porty USB w tym min:   + 1 port USB 3.0 z tyłu obudowy,   + 1 port micro USB z przodu obudowy * 2 port VGA z czego jeden z przodu obudowy * Możliwość rozbudowy o port RS232 |
| **Video** | * Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |
| **Zasilacze** | * Redundantne, Hot-Plug min. 1100W klasy Titanium |
| **Elementy montażowe** | * Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych |
| **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panelu zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. * Możliwość wyłączenia w BIOS funkcji przycisku zasilania. * BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła * Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. * Moduł TPM 2.0 * Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera * Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem * Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). |
| **System operacyjny/dodatkowe oprogramowanie** | * Windows Server Data Center - 2025 – fabrycznie nowy, nigdy wcześniej nieaktywowany na innego użytkownika – na ilość rdzeni zgodnie z zaoferowanymi procesorami. |
| **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 automatycznej rejestracji 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   oraz z możliwością rozszerzenia funkcjonalności o:   * + Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej   + Przesyłanie danych telemetrycznych w czasie rzeczywistym   + Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze   + Automatyczna rejestracja certyfikatów (ACE) |
| **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. |
| **Oprogramowanie do monitorowania** | Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:   * Monitoring:   + ilość podłączonych oraz rozłączonych systemów   + stan podłączonych urządzeń   + informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów   + Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia   + informacje o statusie gwarancji dla poszczególnych urządzeń   + informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń   + informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych.   + Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych   + Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych.   + Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych.   + Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC.   + Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej.   + Monitoring parametrów serwerów z informacją o minimum:     - Obciążeniu procesora     - Zużyciu pamięci RAM     - Temperaturze procesorów     - Temperaturze powietrza wlotowego     - Zużyciu prądu     - Zmianach w fizycznej konfiguracji serwera     - Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.   + Monitoring parametrów pamięci masowych z informacją o minimum:     - Opóźnieniach     - IOPS     - Przepustowości     - Utylizacji kontrolerów     - Pojemność całkowita i dostępna     - Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów.     - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.     - Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata     - Informacje o poziomie redukcji danych     - Informacje o statusie replikacji oraz snapshotów   + Monitoring parametrów przełączników sieciowych z informacją o minimum:     - Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny     - Stanie komponentów: zasilacze, wentylatory     - Podłączonych hostach     - Ilości i statusu portów     - Utylizacji procesora     - Utylizacji poszczególnych portów     - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. * Aktualizacja firmware   + możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania * Raporty   + Możliwość generowania raportów dla serwerów zawierających informację o:     - Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej     - Średnim obciążeniu: procesorów, pamięci RAM, IO,   + Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o:     - Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji   + Generowanie raportów do plików CSV i PDF * Cyberbezpieczeństwo   + Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia.   + Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń.   + Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.   + Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. * Wspierane urządzenia   + Urządzenie Wykonawcy dostarczane w ramach postępowania   + Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) * Wirtualny asystent   + Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; * Możliwość rozszerzenia funkcjonalności   + Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. * Inne   + Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android |
| **Certyfikaty** | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 * Serwer musi posiadać deklarację CE. * Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej [www.epeat.net](http://www.epeat.net) potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku – Wszystkie certyfikaty należy dołączyć do oferty. * 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. |
| **Dokumentacja użytkownika** | * Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim. * Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |
| **Warunki gwarancji** | * Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres min. 24 miesiące. * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. * Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. * Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. * Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. * Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. * Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:   + Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.   + Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.   + Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.   + Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.   + Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. * Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. * Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń. |

**Wymagania w zakresie instalacji i wdrożenia serwerów backupu:**

Zamawiający wymaga:

1. Instalacji sprzętu we wskazanej serwerowni i szafie rack.
2. Instalacji i konfiguracji dostarczonego wraz odpowiednimi urządzeniami systemu operacyjnego Microsoft Windows Server Data Center, podłączenie serwera do wskazanego przez Zamawiającego segmentu sieci.
3. Dołączenia serwerów do wskazanego przez Zamawiającego klastra wirtualizacyjnego.

4. Wykonania migracji maszyn wirtualnych uruchomionych na klastrze wirtualizacyjnym na wskazane serwery, potwierdzenie poprawności pracy.

1. **Macierz dyskowa**

|  |  |
| --- | --- |
| **Element konfiguracji/cecha/funkcjonalność** | **Wymagania minimalne** |
| Typ obudowy | Macierz musi być przystosowana do montażu w szafie rack 19”,  o wysokość maksymalnie 2U z możliwością instalacji min. 24 dysków 2.5” |
| Przestrzeń dyskowa | Zainstalowane:  11x dysk SSD SAS MU o pojemności min. 1.6TB, Hot-Plug |
| Możliwość rozbudowy | Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 276 dysków twardych. |
| Obsługa dysków | Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” jak również 3,5”. |
| Sposób zabezpieczenia danych | Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping).  Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID.  Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku).  Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków. |
| Tryb pracy kontrolerów macierzowych | Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów. |
| Pamięć cache | Macierz musi posiadać sumarycznie minimum 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM.  Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi.  Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat. |
| Rozbudowa pamięci cache | Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash.  Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem. |
| Interfejsy | Macierz musi posiadać, co najmniej 8 portów 12Gb SAS (4 porty na kontroler) |
| Kable/wkładki | 4x kabel 12Gb HD Mini-SAS/HD Mini-SAS min, 2m |
| Zarządzanie | Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej. |
| Zarządzanie grupami dyskowymi oraz dyskami logicznymi | Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej.  Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy.  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Thin Provisioning | Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning.  Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP).  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Tiering | Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS.  Tiering musi obejmować wszystkie woluminy w danej puli dyskowej.  Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych. |
| Wewnętrzne kopie migawkowe | Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii.  Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Wewnętrzne kopie pełne | Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych.  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Migracja danych w obrębie macierzy | Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia. |
| Podłączanie zewnętrznych systemów operacyjnych | Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami).  Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix.  Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych.  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie. |
| Redundancja | Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów.  Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory.  Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.  Zasilacze użyte w macierzy powinny spełniać wymagania dotyczące sprawności dla zasilacza minimum 80+ Gold. |
| Dodatkowe wymagania | Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych.  Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie. |
| Standardy bezpieczeństwa | Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union). |
| Inne | Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym  producenta. Sprzęt musi być produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.  Wszystkie certyfikaty i oświadczenia należy dołączyć do oferty. |
| Warunki gwarancji | Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres min. 24 miesięcy.  Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet.  Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.  Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.  Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki.  Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.  Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.  W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:   * Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. * Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. * Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. * Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. * Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Zamawiającego w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. * Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.   - Posiadanie przez firmę serwisującą ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń. |

Zamawiający wymaga:

1. Instalacji sprzętu we wskazanej serwerowni i szafie rack.
2. Podłączenia macierzy dyskowej do wskazanego segmentu sieci iSCSI.
3. Skonfigurowania woluminów dyskowych i przypisanie ich do serwerów klastra wirtualizacyjnego Hyper-V.
4. Rekonfiguracji zależnych urządzeń/systemów.
5. Migracji danych na woluminy dyskowe nowej macierzy.
6. **Urządzenie do deduplikacji i zabezpieczenia danych – 2 szt.**

Wymagania szczegółowe:

|  |  |
| --- | --- |
| Lp. | Parametr wymagany |
|  |  |
|  | Urządzenie musi być przeznaczone do deduplikacji i przechowywania kopii zapasowych. Urządzenie musi spełniać wymagania wyspecyfikowane w niniejszej tabeli. |
|  | Dostarczone urządzenie musi oferować przestrzeń min. 12TB netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji – przestrzeń dedykowana do gromadzenia deduplikatów, wymagana skalowalność do min. 250TB netto (powierzchni użytkowej widocznej po założeniu systemu plików) |
|  | Dostarczone urządzenie musi umożliwiać rozbudowę o warstwę typu CLOUD dedykowaną do długotrwałego przechowywania danych (tzw. Long Term Retention) – dane o określonej retencji (zgodnie z założoną polityka retencyjną), bez pośrednictwa dodatkowych urządzeń (typu GATEWAY) powinny zostać przemigrowane (w postaci zdeduplikowanej) na dodatkową warstwę, wymagane wsparcie dla dla AWS, Microsoft Azure oraz Google GCP. Wymagana enkrypcja danych przechowywanych na warstwie typu Cloud. Wymagane dostarczenie licencji na przestrzeń min. 80TB netto dla warstwy CLOUD. |
|  | Oferowane urządzenie musi posiadać minimum   * 4 porty 10/25Gb/s Eth OP (wymagana dostawa czterech kabli: 10G 3M Twinax)   wymagana możliwość obsługi każdym z w/w portów protokołów CIFS, NFS, deduplikacja na źródle  wymagana możliwość dodania do w/w konfiguracji portów:   * 4 porty FC 32Gb/s   wymagana możliwość obsługi poprzez porty FC protokołów VTL oraz deduplikacja na źródle  ( możliwość dodania dwóch portów FC oznacza oficjalnie wsparcie takiej konfiguracji przez producenta urządzenia, wolny slot na dodatkowa kartę HBA w przypadku oferowanej konfiguracji urzadzenia oraz możliwość natychmiastowego zamówienia u producenta wymaganej karty rozszerzeń) |
|  | Oferowane urządzenie musi umożliwiać jednoczesny dostęp wszystkimi poniższymi protokołami:   * CIFS, NFS * zapewniającym deduplikację na źródle, wymagane wsparcie dla aplikacji Commvault (co najmniej na poziomie Media Server a także Client Direct przy użyciu storage accelerator), Veeam Backup and Replication (co najmniej na poziomie Veeam Data Mover), NetWorker na poziomie standardowego klienta * VTL (min. 10 jednocześnie) |
|  | Wymagane jest dostarczenie licencji, pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, dedupliakacja na źródle, VTL do oferowanej pojemności urządzenia |
|  | Oferowane pojedyncze urządzenie musi osiągać zagregowaną wydajność (dla maksymalnej konfiguracji) protokołami: **NFS** co najmniej 25 TB/h (dane podawane przez producenta) oraz co najmniej 50 TB/h z wykorzystaniem **deduplikacji na źródle** (dane podawane przez producenta). |
|  | Urządzenie musi pozwalać na jednoczesną obsługę minimum 250 strumieni w tym jednocześnie:   * zapis danych minimum 150 strumieniami * odczyt danych minimum 50 strumieniami * replikacja minimum 50 strumieniami   pochodzących z różnych aplikacji oraz dowolnych protokołów (CIFS, NFS, VTL, deduplikacja na źródle) oraz dowolnych interfejsów (FC, LAN) w tym samym czasie.  Wymienione wartości 250 jednoczesnych strumieni dla wszystkich protokołów (czyli jednocześnie 150 dla zapisu i jednocześnie 50 strumieni dla odczytu i jednocześnie 50 strumieni dla replikacji) musi mieścić się w przedziale oficjalnie rekomendowanym i wspieranym przez producenta urządzenia.  Wszystkie zapisywane strumienie muszą podlegać globalnej deduplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji. |
|  | Oferowane urządzenie musi mieć możliwość emulacji następujących bibliotek taśmowych:   * StorageTek L180 * IBM TS 3500 |
|  | Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych min. LTO5 oraz LTO7 |
|  | Urządzenie musi umożliwiać (w przypadku VTL’a) emulację minimum 250 napędów, emulację min. 30 000 slotów w przypadku poj. biblioteki taśmowej oraz emulację sumarycznie min. 60 000 slotów. |
|  | Oferowane urządzenie musi deduplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia. |
|  | Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku jednak o wielkości nie większej niż 12 kB.  Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych co oznacza, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości, bez konieczności podejmowania czynności mających na celu ustalenie predefiniowanej długości bloków używanych do deduplikacji danych określonego typu. Deduplikacja zmiennym, dynamicznym blokiem oznacza, że wielkość każdego bloku (na jaki są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego oraz jest indywidualnie ustalana przez algorytm deduplikacji zastosowany w urządzeniu, oferowane urządzenie nie może dzielić jakiegokolwiek pojedynczego strumienia danych backupowych na bloki o ustalonej, tej samej długości. |
|  | Oferowany produkt musi posiadać obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, deduplikacja na źródle) przechowywanych w obrębie całego urządzenia co oznacza, że przechowywany na urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany. Wszystkie emulowane jednocześnie w obrębie urządzenia biblioteki wirtualne (VTL) oraz udziały NFS/CIFS również muszą podlegać globalnej deduplikacji – blok danych otrzymany i zapisany w wirtualnej bibliotece „A”, nie może zostać ponownie zapisany jeśli trafi do innej wirtualnej biblioteki „B” w obrębie tego samego urządzenia (to samo dotyczy udziałów NFS/CIFS). Przestrzeń składowania zdeduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych, co oznacza zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych jednocześnie protokołów dostępowych. |
|  | Proces deduplikacji musi odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie zapisane jeszcze na system dyskowy urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych. Wymaganie nie będzie spełnione jeżeli deduplikacja in-line realizowana będzie przez zewnętrzną aplikację backup’ową. Wymaganie deduplikacji in-line dotyczy zapisu danych przez każdy z wymaganych intefejsów, w przypadku interfejsów: NFS, CIFS oraz VTL realizacja deduplikacji in-line nie może w żadnym stopniu zależeć od konkretnej aplikacji backu’owej, dane zapisywane poprzez interfejsy NFS CIFS bez użycia jakiejkolwiek aplikacji backup’owej również muszą być deduplikowane w sposób in-line |
|  | Proponowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej) w celu ich późniejszej deduplikacji (wymagana deduplikacja in-line) |
|  | Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane. |
|  | Tryb zapisu zabezpieczanych danych nie może umożliwiać nadpisywania danych, dane mogą być zapisywane jedynie w trybie append-only, dane dla których wygasła retencja powinny zostać usunięte podczas procesu czyszczenia tzw. Cleaning, wymaganie dotyczy wszystkich danych zapisanych na urządzeniu a nie wybranych grup danych objętych działaniem blokad zabezpieczających przed usunięciem/modyfikacją danych. |
|  | Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje: Commvault, Veeam Backup and Replication, NetWorker.  W przypadku współpracy z każdą z poniższych aplikacji:   * Commvault * Veeam Backup and Replication * NetWorker   urządzenie musi umożliwiać deduplikację na źródle (w przypadku Commvault: co najmniej na poziomie Media Server a także Client Direct przy użyciu storage accelerator, w przypadku Veeam Backup and Replication co najmniej na poziomie Veeam Data Mover), w przypadku NetWorker na poziomie standardowego klienta) i przesłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN.  Deduplikacja w wyżej wymienionych przypadkach musi zapewniać aby do oferowanego urządzenia były transmitowane poprzez sieć LAN jedynie fragmenty danych nie znajdujące się dotychczas na urządzeniu. |
|  | W przypadku przyjmowania backupów z Commvault, Veeam Backup and Replication, NetWorker, urządzenie musi umożliwiać deduplikację na źródle (co najmniej na poziomie Media Server dla CommVault, Data Mover dla Veeam, klienta dla NetWorker) i przesłanie nowych, nieznajdujących się jeszcze na urządzeniu bloków poprzez sieć FC.  Deduplikacja w wyżej wymienionych przypadkach musi zapewniać aby do oferowanego urządzenia były transmitowane poprzez sieć FC jedynie fragmenty danych nie znajdujące się dotychczas na urządzeniu. |
|  | Oferowane urządzenie musi umożliwiać uruchamianie maszyn wirtualnych VMware bezpośrednio z danych backupowych bez konieczności odtwarzania danych. |
|  | Wymagana funkcjonalność Load Balancing oraz Link Failover w obrębie portów (Eth) wykorzystywanych przez aplikację backupową. |
|  | Wymagane wsparcie dla backupów typu Virtual Synthetics w przypadku aplikacji Commvault, Veeam Backup and Replication oraz NetWorker. |
|  | W przypadku deduplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów. |
|  | Urządzenie musi umożliwiać zaszyfrowanie przechowywanych danych, wymagane licencje umożliwiające zaszyfrowanie i przechowywanie zaszyfrowanych danych w obrębie maksymalnej pojemności oferowanego urządzenia. |
|  | Urządzenie musi wspierać deduplikację na źródle poprzez sieć FC (SAN) minimum dla następujących systemów operacyjnych:   * Windows * Linux (RedHat, SuSE) |
|  | Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego urządzenia takiego samego typu. Konfiguracja replikacji musi być możliwa w każdym z trybów:  \* jeden do jednego  \* wiele do jednego  \* jeden do wielu  \* kaskadowej (urządzenie A replikuje dane do urządznia B, które te same dane replikuje do urządzenia C).  Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu. Ewentualna licencja na replikację jest przedmiotem postępowania. |
|  | Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji. |
|  | W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami. |
|  | W przypadku replikacji danych między dwoma urządzeniami oferowanego typu, wymagana możliwość kontroli przez: Commvault oraz NetWorker muszą być możliwe do uzyskania jednocześnie wszystkie następujące funkcjonalności:   * replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących * replikacji podlegają tylko te fragmenty danych (na poziomie bloków używanych do deduplikacji), które nie znajdują się na docelowym urządzeniu * replikacja zarządzana jest z poziomu wymaganej aplikacji * aplikacja posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji |
|  | Oferowane urządzenie musi działać poprawnie przy zapełnieniu danymi na poziomie co najmniej 90%. Dokumentacja urządzenia nie może wskazywać na ew. problemy, obostrzenia, które są efektem zapełnieniu urządzenia zabezpieczanymi danymi, na poziomie mniejszym niż 90%. |
|  | Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami – oferowane urządzenie musi być wyposażone w mechanizm umożliwiający zarządzaniem stopnia wykorzystania pasma na potrzeby replikacji. |
|  | Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 bądź równoważnej. |
|  | Oferowane urządzenie musi pozwalać na realizację oraz przechowywanie SnapShot’ów, czyli umożliwiać zamrożenie obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze Snapshot’u.  Odtworzenie danych ze Snapshot’u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania/odtwarzania backupów). |
|  | Urządzenie musi pozwalać na przechowywanie minimum 500 Snapshotów jednocześnie w obrębie oferowanej przestrzeni, przy zachowaniu globalnej deduplikacji oraz standardowego trybu pracy urządzenia – umożliwiającego wykorzystanie wszystkich dostępnych funkcjonalności. |
|  | Urządzenie musi umożliwiać podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą deduplikowane (globalna deduplikacja między logicznymi częściami urządzenia). |
|  | Urządzenie musi mieć możliwość podziału na minimum 10 logicznych części pracujących równolegle. Producent musi oficjalnie wspierać pracę minimum 10 logicznych części pracujących równolegle z pełną wydajnością urządzenia. |
|  | Dla każdej z w/w logicznych części oferowanego urządzenia musi być możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią deduplikatora. Użytkownicy zarządzający logiczną częścią A muszą widzieć tylko i wyłącznie zasoby logicznej części A i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia. |
|  | Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia dostępnego za pośrednictwem:   * CIFS * NFS * VTL * deduplikacja na źródle |
|  | Urządzenie musi umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalność WORM). Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem pliku, modyfikacją pliku.  Blokada skasowania danych musi działać w dwóch trybach (do wyboru przez administratora):   1. Możliwość zdjęcia blokady przed upływem ważności danych 2. Brak możliwości zdjęcia blokady przed upływem ważności danych (COMPLIANCE), w tym wypadku wymagane wsparcie norm SEC 17a-4(f) oraz ISO Standard 15489-1 w zakresie ochrony danych, wymagane oficjalne wsparcie wymaganej blokady przez aplikację Commvault, Veeam Backup and Replication oraz NetWorker – wymagane potwierdzenie na oficjalnych stronach w/w aplikacji backup’owych oraz producenta oferowanego deduplikatora.   Licencje na blokadę usunięcia/zmiany przechowywanych plików muszą być dostarczone wraz z urządzeniem.  Wymagana możliwość automatycznego uruchamiania blokady (podczas zapisu) WORM dla danych zapisywanych na obszar objęty działaniem wspomnianej blokady. W każdym przypadku wymagana również możliwość używania blokady WORM dla obrazu danych uzyskanych poprzez użycie wymaganej funkcjonalności SnapShot. |
|  | Urządzenie musi mieć możliwość przechowywania danych niezmienialnych:   * Video * Grafika * Nagrania dźwiękowe * Pliki pdf   na udziałach CIFS/NFS. |
|  | Urządzenie musi weryfikować dane po zapisie (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie ale o weryfikację wszystkich zabezpieczanych danych backup’owych). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie. Powyższa weryfikacja musi być realizowana w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), musi być realizowana w trybie ciągłym (a nie ad-hoc), wymagane parametry wydajnościowe urządzenia muszą uwzględniać tę funkcjonalność. Wymagane potwierdzenie opisanej funkcjonalności w oficjalnej dokumentacji producenta oferowanego urządzenia. |
|  | Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia. |
|  | Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu). |
|  | Wymagana możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora), wymagane potwierdzenie w ogólno dostępnej dokumentacji. |
|  | Wymagana możliwość zdefiniowania harmonogramu wg. którego wykonywany jest proces usuwania przeterminowanych danych (czyszczenia), realizowany równolegle z procesami backup/restore/replication. |
|  | Standardowa częstotliwość usuwania przeterminowanych danych (czyszczenie) nie powinna być większa niż 1 raz na tydzień - minimalizując czas w którym backupy/odtworzenia narażone są na spowolnienie (weryfikacja wymagania na podstawie dokumentacji typu DOBRE PRAKTYKI publikowanej przez producenta). |
|  | Urządzenie musi umożliwiać systemowo (wbudowana funkcjonalność) - realizację procesu pierwszego czyszczenia dopiero po przekroczeniu 75% zajętości oferowanej przestrzeni. |
|  | Urządzenie musi mieć możliwość zarządzania poprzez   * Interfejs graficzny dostępny z przeglądarki internetowej * Poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell) |
|  | Oprogramowanie do zarządzania musi rezydować na oferowanym urządzeniu deduplikacyjnym. |
|  | Oferowane urządzenie musi mieć możliwość sprawdzenia pakietu upgrade’ującego firmware urządzenia (GUI lub CLI), to znaczy sprawdzenia czy nowa wersja systemu nie spowoduje problemów z urządzeniem. |
|  | Urządzenie musi być rozwiązaniem kompletnym, appliancem sprzętowym pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway. |
|  | Oferowane urządzenie musi być objęte min. 4-letnim wsparciem producenta działającym w trybie zgłaszania awarii: 24x7 oraz reakcją NBD. Uszkodzone nośniki pozostają u Zamawiającego bez ponoszenia dodatkowych kosztów. |
|  | Oferowane urządzenie musi być wyprodukowane zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001  Oferowane urządzenie musi posiadać deklarację CE.  Wszystkie certyfikaty należy dołączyć do oferty. |

1. **Oprogramowanie do zarządzania klastrem i systemem bazodanowym (wykonywania kopii zapasowych) – 1 sztuka**

Wymagania ogólne:

• Dostarczone oprogramowanie musi umożliwiać wykonywanie kopii zapasowych z minimum 20 maszyn wirtualnych pracujących w środowisku wirtualizacyjnym lub 20 serwerów fizycznych, każdy z własną instancją systemu operacyjnego.

• Dostarczone oprogramowanie musi być objęte wsparciem technicznym producenta przez okres 24 miesięcy.

• Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5.

• Oprogramowanie musi współpracować z infrastrukturą Vmware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.

• Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.

Wymagania funkcjonalne:

• Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej

• Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków

• Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji

• Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.

• Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych takiej puli.

• Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.

• Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.

• Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania

• Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time)

• Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu

• Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API

• Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji

• Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji

• Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania

• Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

• Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej

• Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np. skasowanie backupu, dodanie kolejnego administratora)

• Oprogramowanie musi posiadać integracje z systemami zarządzania kluczami szyfrującymi (KMS)

• Oprogramowanie musi posiadać integracje z systemami typu SIEM

• Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.

Wymagania RPO:

• Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej

• Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.

• Oprogramowanie musi oferować możliwość sterowania obciążeniem storage’u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru

• Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku Vmware.

• Oprogramowanie musi posiadać wsparcie dla Vmware vSAN potwierdzone odpowiednią certyfikacją Vmware.

• Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592).

• Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)

• Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum Dxi oraz Infinidat InfiniGuard.

• Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.

• Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.

• Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury Vmware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.

• Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o Vmware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury Vmware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.

• Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik

• Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)

• Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN).

Wymagania RTO:

• Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk Vmware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych.

• Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)

• Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności – oprogramowanie musi realizować taką migrację swoimi mechanizmami

• Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre

• Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.

• Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków

• Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.

• Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików

• Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy Vmware i PowerShell Direct dla platformy Hyper-V.

• Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell

• Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM

• Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.

• Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł.

• Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze „Permanently Deleted Objects”). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.

• Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.

• Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.

• Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.

• Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.

• Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji

• Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN

• Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle

• Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI

• Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2

• Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym „reverse CBT” oraz odtwarzanie z wykorzystaniem sieci SAN

Ograniczenie ryzyka:

• Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)

• Dla Vmware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.

• Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem

• Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.

• Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware

• Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania

• Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków

• Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

Środowiska fizyczne:

• Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego

• Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych

• Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE

• Rozwiązanie musi wspierać system operacyjny macOS

• Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix

• Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)

• Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster

• Rozwiązanie musi wspierać zabezpieczanie do odzyskiwania z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów

• Rozwiązanie musi wspierać backup podłączonych dysków USB

• Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym

• Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury)

• Rozwiązanie musi wspierać deduplikację oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone

• Rozwiązanie musi wspierać kontrolę pasma sieciowego

• Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych

• Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN

• Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft

• Rozwiązanie musi wspierać technologię BitLocker

• Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania

• Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych

• Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych

• Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle I PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu.

• Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform

• Rozwiązanie musi wspierać szyfrowanie

• Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne

• Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego

• Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej

• Rozwiązanie musi wspierać tworzenie wielu zadań backupowych

Monitoring

• System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na Vmware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich

• System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Vmware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie

• System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.

• System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter

• System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn

• System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel

• System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk

• System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora

• System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów

• System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)

• System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna

• System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego

• System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta

• System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.

• System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.

• System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware

• System musi mieć możliwość monitorowania instancji Vmware vCloud Director w wersji od 10.x do 10.4

Raportowanie

• System musi umożliwiać raportowanie środowiska wirtualizacyjnego Vmware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie

• System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.

• System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.

• System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V

• System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF

• System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc

• System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach

• System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów

• System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych

• System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych

• System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury

• System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta

• System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.

• System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.

• System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware

• System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)

• System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie.

**Urządzenie do deduplikacji i zabezpieczenia danych, Oprogramowanie do zarządzania klastrem i systemem bazodanowym (wykonywania kopii zapasowych)**

Zamawiający wymaga:

1. Instalacji sprzętu we wskazanej serwerowni i szafie rack.
2. Instalacji i konfiguracji dostarczonego wraz odpowiednimi urządzeniami systemu operacyjnego Microsoft Windows Server, podłączenie serwera do wskazanych przez Zamawiającego segmentów sieci.
3. Skonfigurowanie połączenia serwera backupu z urządzeniem do deduplikacji.
4. Instalacji oprogramowania do wykonywania kopii zapasowych na serwerze backupu.
5. Skonfigurowania serwera backupu jako serwera kopii zapasowych dla wskazanego przez Zamawiającego, istniejącego środowiska wirtualizacyjnego, w tym:
   1. skonfigurowanie repozytorium danych na dyskach wewnętrznych serwera backupu oraz repozytorium danych na urządzeniu do deduplikacji,
   2. zdefiniowanie zadań i harmonogramów kopii zapasowych dla serwerów wirtualnych z uwzględnieniem odtworzenia całej maszyny wirtualnej, jak i granularnego odtwarzania pojedynczych plików lub aplikacji z danej maszyny wirtualnej, wykonanie testowego odtwarzania danych
6. **Zasilacz do serwerów (UPS) Typ 1 – 2 szt.**

Zasilacz awaryjny powinien spełniać następujące wymagania (wymagania te mają charakter minimalny):

Wymagania ogólne

* Moc pozorna: min. 6000VA
* Moc rzeczywista: min. 6000W
* Technologia on-line (VFI), podwójna konwersja
* Sprawność max (dla VFI) ˃ 95 %
* Typ obudowy: rack/tower

Praca sieciowa

zakres napięcia wejściowego: 110V – 275V

zakres częstotliwości napięcia wejściowego: 45 - 55 Hz / 54 - 66 Hz

Zakres napięcia wyjściowego: 208 V AC / 220 V AC / 230 V AC / 240 V AC - domyślnie 230 V AC

Wartość napięcia wyjściowego ustawiana z panelu LCD: Tak

Kształt napięcia wyjściowego: sinusoidalny

Czas przełączania sieć: UPS 0ms

Współczynnik odkształceń prądu wejściowego THDi < 3%

Praca bateryjna

Napięcie wyjściowe ~230V ± 1%

Częstotliwość napięcia wyjściowego 50Hz/60Hz ± 0,1Hz

Kształt napięcia wyjściowego na pracy bateryjnej: sinusoidalny

Zabezpieczenie przeciwzwarciowe gniazd wyjściowych: bezpiecznik automatyczny 20A

Zabezpieczenie przeciążeniowe: elektroniczne

Akumulatory w UPS: nie

Akumulatory w Modułach Bateryjnych: minimum 20x 12V 9Ah; szczelne, bezobsługowe

Czas podtrzymania UPS + 1 szt. Modułu Bateryjnego dla obciążenia 6000W / 5000W / 4000W – odpowiednio:

Minimum: 6 /9/13 min

Przeciążalność:

100%＜obciążenie ≤105%: ciągłe

105%＜obciążenie ≤125%: 10 minut

125%＜obciążenie ≤150%: 30s

>150% : 500ms

Wejście zasilania: Listwa zaciskowa

Ilość i typ gniazd wyjściowych:

Minimum 2x IEC 320 C13 (10 A) + listwa zaciskowa + dodatkowy moduł PDU wyposażony w minimum 2x IEC 320 C13 (10 A) + 1x IEC 320 C19 (16A) niesterowalne oraz 2x IEC 320 C13 (10 A) + 1x IEC 320 C19 (16A) sterowalne;

Sygnalizacja

* Wyświetlacz LCD (informacje wskazujące pracę sieciową, bateryjną, przeciążenie i ładowanie akumulatora).
* Diody LED

Pozostałe:

* Możliwość podłączenia dodatkowych, zewnętrznych modułów bateryjnych
* Wymagana możliwość podłączenia minimum 5 zewnętrznych modułów bateryjnych
* Interfejs komunikacyjny: RS232, USB HID, karta SNMP/http - wymagana na wyposażeniu
* Złącze EPO: wymagane NC
* Styki bezpotencjałowe zamontowane na stałe w obudowie UPS: wymagany minimum 1x wejściowy i 1x wyjściowy - wymagane na wyposażeniu
* Waga UPSa do 14,5 kg
* Waga pojedynczego modułu bateryjnego: do 69 kg
* Wymiary UPS - wersja RACK nie większe niż: wysokość 86mm; szerokość 438mm; głębokość 576mm
* Wymiary modułu bateryjnego - wersja RACK: nie większe niż: wysokość 130mm; szerokość 438mm; głębokość 596mm
* Łączna wysokość w szafie RACK 19" dla oferowanego zestawu: nie więcej niż 8U

Gwarancja i dokumenty

* min. 24 miesiące na elektronikę i min. 24 miesiące na akumulatory.
* Wymagane dołączenie do oferty:
  + Certyfikaty producenta: ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania. Wszystkie certyfikaty należy dołączyć do oferty.

Serwis

* autoryzowany serwis producenta zlokalizowany w Polsce.
* serwis realizowany w systemie door to door
* wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów w okresie gwarancji.

Oprogramowanie

* oprogramowanie tego samego producenta co UPS, w języku polskim do zarządzania i monitorowania pracy UPS dla Windows, Linux oraz systemów wirtualizacji VMware, Hyper-V, Citrix XenServer bez ograniczeń co do ilości monitorowanych stanowisk (bez dodatkowych opłat za licencje)
* możliwość edycji nazw urządzeń na liście monitorowanych UPSów

1. **Zasilacz do stacji końcowych Typ 2 – 15 szt.**

Wymagania ogólne:

**•** Moc pozorna: min. 1200VA

• Moc rzeczywista: min. 600VA

• Topologia: VI (line interactive)

• Typ obudowy: Wolnostojąca

• Napięcie wejściowe: 170 ÷ 280 V AC ± 7 %

• Częstotliwość napięcia wejściowego: 45 ÷ 55 Hz ± 1 Hz

• Zakres napięcia wyjściowego: 230 V AC ± 10 %

• Czas przełączania sieć – UPS: <6ms

• Schodkowa aproksymacja sinusoidy / Tak jak na wejściu

• Napięcie wyjściowe: ~230V ± 10%

• Częstotliwość napięcia wyjściowego: 50Hz ± 1Hz

• Kształt napięcia wyjściowego na pracy bateryjnej: Schodkowa aproksymacja sinusoidy

• Zabezpieczenie wyjściowe przeciwzwarciowe/ przeciążeniowe: elektroniczne

• Czas podtrzymania (P 0,8max/P 0,5max): minimum 4/10 min

• Akumulatory wewnętrzne: minimum 2szt 12V7Ah; szczelne, bezobsługowe

• Wejście zasilania: Przewód zasilający CEE7/7 – IEC 320 C13, 10A

• Ilość i typ gniazd wyjściowych: minimum 2x PN-E-93201 + 2x IEC320 C13 (10A)

• Filtr telekomunikacyjny/teleinformatyczny: minimum filtr teleinformatyczny RJ-45 (LAN 10/100 Base-T)

• Sygnalizacja: Akustyczno-optyczna, w tym minimum wyświetlacz LCD sygnalizujący napięcie wejściowe i wyjściowe, poziom obciążenia, stan naładowania baterii oraz aktywność systemu AVR

• Zimny start: tak

• Interfejs komunikacyjny: USB (kabel w komplecie)

• Waga UPS: do 9kg

Gwarancja i dokumenty:

* min. 24 miesiące na elektronikę i min. 24 miesiące na akumulatory.
* Wymagane dołączenie do oferty:
* Certyfikaty producenta: ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania. Wszystkie certyfikaty należy dołączyć do oferty.

Serwis:

* Serwis: autoryzowany serwis producenta zlokalizowany w Polsce. Serwis realizowany w systemie door-to-door
* Oprogramowanie producenta w języku polskim do zarządzania i monitorowania pracy UPS .
* Wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów w okresie gwarancji.
* Wsparcie dla systemów Linux, Windows oraz wirtualizacji Hyper-V, Vmware, XenServer

1. **Wymagania ogólne w zakresie instalacji, wdrożenia oraz konfiguracji sprzętu i oprogramowania:**

Zamawiający wymaga:

1. Opracowania projektu technicznego wdrożenia, w konsultacji z Zamawiającym.
2. Zaktualizowania oprogramowania/sterowników/firmware dla wszystkich wdrażanych rozwiązań do najnowszej dostępnej w dniu wdrożenia i stabilnej wersji (wymaganie to dotyczy również infrastruktury zależnej, współpracującej z wdrażanymi rozwiązaniami).
3. Realizacji prac wdrożeniowych przez osoby posiadające certyfikaty producentów wdrażanych rozwiązań.
4. Realizacji prac wdrożeniowych, które będą skutkowały niedostępnością środowiska IT Zamawiającego, w godzinach 20:00 – 5:00 w dni od poniedziałku do piątku lub w sobotę i niedzielę przez cała dobę i planowane w uzgodnieniu z Zamawiającym z minimum trzydniowym wyprzedzeniem.
5. Opracowania dokumentacji powykonawczej wdrożenia, obejmującej całość wykonanych prac oraz zmiany wprowadzone w infrastrukturze zależnej.