Załącznik nr 11 do SWZ - OPZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Zakup i dostawa sprzętu komputerowego na potrzeby Miejsko-Gminnego Ośrodka Pomocy Społecznej w Jelczu-Laskowicach

1. **Przedmiotem zamówienia jest dostawa sprzętu komputerowego, tj.:**

– 1. Serwer z oprogramowaniem systemowym i licencjami dostępowymi dla użytkowników
– 2. Urządzenie NAS do archiwizacji z dyskami,
– 3. Oprogramowania do wykonywania kopii zapasowych, Licencja do oprogramowania do wykonywania kopii zapasowych 30 sztuk (na dwa lata)
–

Zamawiany sprzęt ma być kompatybilny z posiadaną przez Zamawiającego infrastrukturą i systemami. tj:

- - Windows Serwer 2019
- - Windows 10/11

W Specyfikacji produktów (załącznik nr 1A do SWZ) należy podać model, typ i nazwę producenta oferowanego sprzętu. W razie wątpliwości zamawiający może wezwać do przedstawienia kart technicznych produktów.

Oferowany sprzęt musi być jednorodny, tj. model, typ i producent musi być taki sam dla poszczególnych rodzajów sprzętu.

2. **Minimalne wymagane parametry techniczne dla sprzętu komputerowego:**

Nazwa	Wymagane minimalne parametry techniczne
1.	**Serwer -1 sztuka**
Obudowa	Obudowa Rack o wysokości max. 1U umożliwiającą instalację min. 8 dysków 2,5" z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.
Płyta główna	Płyta główna z możliwością zainstalowania 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	Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.8GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 127 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
RAM	Min. 32GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Zabezpieczenia pamięci RAM	Advanced ECC, Memory Health Check, Memory Page Retire
Gniazda PCIe	- minimum 2 sloty PCIe x16 generacji min. 3
Interfejsy sieciowe/FC/SAS	Zintegrowana z płytą główną karta sieciowa 2 x 1Gb Ethernet Wbudowane cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT, Karta sieciowa nie może zajmować slotu PCIe Możliwość instalacji wymiennie modułów udostępniających: - min. dwa interfejsy sieciowe 10Gb Ethernet w standardzie BaseT - min. cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT - min. dwa interfejsy sieciowe 25Gb Ethernet ze złączami SFP28

Dyski twarde	Zainstalowany 2 x 480GB SSD SATA o DWPD co najmniej 3 Zainstalowane 5 x 2.4TB SAS 10k Możliwość instalacji dwóch dysków hot-swap M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1.
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samo szyfrujących.
Wbudowane porty	min. port USB 2.0 oraz port USB 3.0, port VGA.
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug min. 700W o klasie efektywności co najmniej Titanium
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 v3 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
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: · zdalny dostęp do graficznego interfejsu Web karty zarządzającej · szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika · możliwość podmontowania zdalnych wirtualnych napędó · wirtualną konsolę z dostępem do myszy, klawiatury · wsparcie dla IPv6 · wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH · możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz. · możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer · integracja z Active Directory · możliwość obsługi przez ośmiu administratorów jednocześnie · Wsparcie dla automatycznej rejestracji DNS · wsparcie dla LLDP · wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej · możliwość podłączenia lokalnego poprzez złącze RS-232. · możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy. · Monitorowanie zużycia dysków SSD · możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi, · Automatyczne zgłaszanie alertów do centrum serwisowego producenta · Automatyczne update firmware dla wszystkich komponentów serwera · Możliwość przywrócenia poprzednich wersji firmware · Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON · Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych · Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram. · Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera · Serwer musi posiadać możliwość uruchomienia funkcjonalności umożliwiającej 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 lub WIFI.
System Operacyjny	Zakres Przedmiotu Zamówienia obejmuje dostarczenie i wdrożenie Oprogramowania Windows Server 2022 Standard,16CORE 3 x 10-pack of Windows Server 2022/2019 User CALs 10 x Microsoft SQL Server 2022 Standard, USER CALs 1 x Microsoft SQL Server 2022 Standard lub równoważny współpracujący z posiadanym przez Zamawiającego oprogramowaniem Windows Serwer 2019 i SQL
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001 lub równoważną. Serwer musi posiadać deklaracja CE. Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 lub oświadczenie producenta o stosowaniu w fabrykach polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows 2016, Microsoft Windows 2019 x64, Microsoft Windows 2022.
Normy Środowiskowe	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 wraz z ofertą dokument potwierdzający spełnianie wymogu.*** Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych **w postaci oświadczenia producenta serwera** (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych", pkt 3.4.2.1; dokument z grudnia 2006 r.), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gr - ***Wykonawca złoży wraz z ofertą dokument potwierdzający spełnianie wymogu.***
Warunki gwarancji	Min. trzy lata gwarancji producenta czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską infolinię telefoniczną producenta. W razie awarii dyski pozostają własnością zamawiającego. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. **Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta – wymagane do umowy.** • Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji systemu.
2.	**Dysk sieciowy – 1 sztuka**
Procesor	Procesor 64 bit x86 o taktowaniu nie mniejszym niż 3.3 GHz

Procesor liczba rdzeni	Nie mniej niż 6
Zintegrowany układ graficzny	Wymagany
Pamięć RAM	Nie mniej niż 16 GB DDR4 ECC
Pamieć RAM liczba slotów	Minimum 4 sloty
Pamięć RAM - możliwość rozszerzenia	Nie mniej niż do 128GB
Pamięć Flash	Nie mniej niż 5 GB
Liczba zatok na dyski	Minimum 12 (w tym minimum 8 zatok 3,5")
Obsugiwane dyski w zatokach 3,5"	3.5" SATA oraz 2.5" SATA oraz 2.5" SATA SSD
Pojemność dysków twardych	do 20TB zainstalowane dyski 8 x 8TB, zgodne z wymaganiami producenta dysku sieciowego
Możliwość podłączenia modułu rozszerzającego	Tak, co najmniej 2
Porty LAN 2,5 Gb/s	Minimum 4 szt. RJ-45
Porty LAN 10 Gb/s	Minimum 2 szt. RJ-45
Diody LED	Minimum Status, LAN, HDD
Porty USB 3.2 Gen2	Minimum 4, w tym 2 typu C
Gniazdo PCiE	Tak, minimum 3 Gen3 w tym minimum 2 wolne gniazda
Przyciski	Reset, Zasilanie
Typ obudowy	Tower
Dopuszczalna temperatura pracy	od 0 do 40˚C
Wilgotność względna podczas pracy	5-95% R.H.
Zasilanie	Max. 600 W
Specyfikacja oprogramowania	
Obsługa dwóch systemów operacyjnych	Możliwość wyboru w trakcie inicjalizacji urządzenia systemu operacyjnego opartego na systemach plików EXT4 lub ZFS
Wymagania dla systemu operacyjnego opartego o system plików EXT4	
Agregacja łączy	Tak

Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+
Możliwość podłączenia karty WLAN na USB	Tak
Szyfrowanie udziałów	Tak, min AES 256
Szyfrowanie dysków zewnętrznych	Tak
Zarządzanie dyskami	Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek Obsługa replikacji migawek
Wbudowana obsługa iSCSI	Multi-LUNs na Target Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN
Zarządzanie prawami dostępu	Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL
Obsługa Windows AD	Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa plików producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,
Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box
Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer Dostępne na systemy iOS oraz Android
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu

VPN	VPN client / VPN server Obsługa PPTP, OpenVPN
Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania automatyczna Możliwość aktualizacji oprogramowania ręcznie Ustawienia systemu: Kopia, Przywracanie, Resetowanie
Wirtualizacja	Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android. Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5 Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych.
Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker
Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP (tylko admin) Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek
Gwarancja	min. 3 lata
3.	**OPROGRAMOWANIE DO ARCHIWIZACJI**

Zarządzanie i magazyny

1. Produkt dostępny w polskiej wersji językowej.
2. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej
3. System musi umożliwiać tworzenie kopii zapasowych na poziomie dysków
4. System musi umożliwiać tworzenie kopii zapasowych na poziomie plików i folderów
5. System musi umożliwiać replikację kopii zapasowych do wielu lokalizacji docelowych
6. System musi umożliwiać tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT
7. System musi umożliwiać współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft
8. Możliwość zdefiniowania limitu przepustowości sieciowej z jakiej ma korzystać oprogramowanie backupowe
9. System zarządzania nie może być oparty o relacyjne bazy danych.
10. Rozwiązanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej).
11. Rozwiązanie 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).

12. Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania, ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych.
13. Rozwiązanie musi być systemem multi-storage-owym i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako przestrzeń do replikacji danych.
14. System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.
15. Rozwiązanie w warstwie sprzętowej powinno bazować na standardowych komponentach architektury x86, bez powiązania i poleganiu na komponentach wyłącznie jednego dostawy (tzw. "no propietary vendor lock").
16. System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami.
17. System musi umożliwiać wykonywanie kopii obrazu dysku, kopii plików i katalogów oraz kopii maszyn wirtualnych bez ich zatrzymywania z zachowaniem stuprocentowej integralności i spójności danych wewnątrz wykonanej kopii zapasowej.
18. Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie.
19. Rozwiązanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.
20. System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu.
21. Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych
22. Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS.
23. System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego.
24. System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii).
25. Rozwiązanie musi udostępniać możliwość podglądu postępu działania dowolnego zadania, w tym zadania wykonywania kopii zapasowych, odtwarzania danych, testowego odtwarzania danych, usuwania danych oraz zadania odświeżania zajętości magazynu na dane.
26. Rozwiązanie musi posiadać system powiadamiania poprzez e-mail oraz Slack 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.
27. System powinien umożliwiać wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika,
28. Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta.
29. Rozwiązanie musi być wyskalowane, dobrane pod względem wymaganej funkcjonalności i wydajności stosownie do ilości zabezpieczanych danych i obiektów z uwzględnieniem przyrostu danych (serwery, maszyny wirtualne, bazy danych itp.) zgodnie z opisem w zapytaniu ofertowym.
30. Wydajność oferowanej konfiguracji musi być taka, aby wszystkie funkcje systemu były dostępne w chwili wdrożenia (np. deduplikacja, kompresja, instancja workerów i browserów, replikacja, testowe odtwarzanie maszyn wirtualnych).
31. System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych.
32. Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów.
33. Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych z deduplikowanych
34. Proces deduplikacji nie może posiadać pojedynczego punktu awarii, tym samym musi być dostępny jednocześnie na każdym wspieranym magazynie na dane - również replikacyjnych. Awaria jednego z magazynów na dane nie może wpłynąć na integralność deduplikatów, jak i tablicy deduplikatów na innym magazynie.
35. Proces deduplikacji realizowany jest blokiem o stałej wielkości, którego wielkość może zostać ustalona na etapie wdrożenia rozwiązania zgodnie z najlepszymi praktykami producenta.
36. Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego.
37. Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki.
38. Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu.
39. System musi pozwalać na automatyczne aktualizacje oprogramowania.
40. System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS.
41. System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS w celu ich zabezpieczenia.
42. System tworzenia kopii zapasowej musi przechowywać dane w sposób zapewniający ich niezmienność (tzw. "resilience"), dzięki czemu kopie zapasowe nie będą mogły zostać nadpisane lub zmodyfikowane przez cały okres ich przechowywania, retencji.
43. System zarówno będzie przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu również musi być szyfrowany.
44. Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego

samego interfejsu użytkownika, co inne przywracanie dane.

45. System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników.
46. System musi pozwalać na gradację uprawnień administratorów - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: system operator, backup operator, restore operator, viewer. Dla każdej z tych ról system musi umożliwiać przypisywanie dodatkowych uprawnień, w tym możliwość zablokowania usuwania danych.
47. Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w momencie spełnienia dodatkowych wymogów.
48. W sytuacji, gdyby podstawowe urządzenie tworzenia kopii zapasowej było niedostępne, system musi posiadać możliwość przywrócenia z archiwum za pomocą innej instancji systemu dostarczonej przez tego samego producenta. tzn. archiwum musi zawierać wszystkie informacje konieczne do odzyskania.
49. Rozwiązanie musi umożliwiać uruchomienie konsoli w chmurze producenta zlokalizowanej na terenie Polski, w celu umożliwienia dostępu do środowiska zarządzania kopiami zapasowymi w przypadku czasowej niedostępności środowiska lokalnego.
50. System kopii zapasowej musi umożliwiać dostęp do konsoli administracyjnej z wielu stacji roboczych.
51. System kopii zapasowej musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
52. System powinien posiadać predefiniowane schemat tworzenia kopii zapasowych: Custom, Basic, G-F-S, Forever incremental,
53. Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC).
54. Możliwość składowania utworzonych kopii zapasowych na magazynach chmurowych Amazon AWS, Azure, Wasabi, Google Cloud Storage, Backblaze B2, magazyny zgodne z S3.
55. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych po protokole smb, nfs, iscsi, katalog lokalny
56. Zarządzanie i odzyskiwanie danych z kopii musi odbywać się z tego samego interfejsu użytkownika (konsoli), niezależnie od tego, gdzie znajduje się kopia zapasowa (w chmurze AWS, Azure, GCP, w Data Center czy w usłudze typu SaaS).
57. Czas przechowywania kopii zapasowej (retention time) systemu backupu nie może być zmieniony np. poprzez manipulowanie wskazaniami zegara serwera NTP w celu szybszego ich wyekspirowania - tzn. czasy przechowywania kopii zapasowych nie będą zależne od wskazań zegara czasu serwera NTP, ale będą wykorzystywać technologię, która mierzy upływ czasu.
58. Możliwość generowania raportów dobowych w oparciu o harmonogram
59. Produkt musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (datacenter musi być zlokalizowane na terenie Polski)
60. Produkt musi posiadać możliwość zdefiniowania maksymalnej liczby równocześnie backupowanych urządzeń w ramach jednego planu backupowego, niezależnie od typu urządzenia (np. stacja robocza, serwer, maszyna wirtualna)
61. Możliwość wyświetlenia szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM, System operacyjny, Adres IP.
62. Produkt musi posiadać możliwość zdefiniowania poziomu obciążenia magazynu, po osiągnięciu którego zostanie wysłane powiadomienia e-mail. (poziom definiowany indywidualnie dla każdego magazynu)

Wspierane systemy

Możliwość instalacji oraz uruchomienia agenta backupowego na hostach fizycznych, maszynach wirtualnych, czy też kontenerach docker opartych o systemy:

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 2016+,
VMware: 6.7+.

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: 2012 R2+,

Środowiska fizyczne i bazy danych

1. Rozwiązanie powinno umożliwiać tworzenie grup urządzeń w celu automatyzacji procesów podczas pracy z urządzeniami.
2. Produkt musi posiadać możliwość tworzenia zadań dla grupy urządzeń oraz dla wybranych urządzeń.
3. Rozwiązanie musi pozwalać na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej.
4. Rozwiązanie backupowe musi pozwalać na zabezpieczanie zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption.
5. System jest niezależny od wersji Microsoft SQL i musi umożliwiać przywracanie danych SQL dla tej samej lub nowszej wersji.
6. System musi obsługiwać również narzędzia RMAN firmy Oracle do tworzenia kopii zapasowych i odzyskiwania. Dodatkowo system musi obsługiwać funkcję przyrostowego scalania danych.
7. System kopii zapasowej musi wspierać odtwarzanie pojedynczych plików z systemów Windows oraz Linux.
8. W przypadku niedostępności źródła danych, system musi oczekiwać na powrót dostępności źródła danych przez określony przez administratora okres. W przypadku braku powrotu dostępności źródła, system musi podjąć ustaloną przez administratora liczbę prób kontynuacji kopii. W przypadku powrotu źródła danych system musi kontynuować zadanie backupu od momentu, w którym wystąpiła niedostępność źródła - system nie może rozpoczynać zadania od punktu początkowego i rozpoczynać przesyłania kopii od zera. W przypadku braku powrotu źródła danych system powinien zakończyć zadanie błędem.
9. Odtwarzanie Bare Metal Restore w Systemie 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.
10. Rozwiązanie powinno umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego bootowalnego nośnika danych.
11. Rozwiązanie powinno wspierać odtwarzanie danych w scenariuszach P2P, P2V, V2P, V2V.
12. Rozwiązanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK).
13. Rozwiązanie musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) oraz z prawami dostępu. Funkcjonalność ta musi być możliwa do skonfigurowania przez administratora na etapie konfiguracji procesu przywracania danych.
14. Rozwiązanie musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows).

Środowiska wirtualne

1. System musi wspierać kopię w trybie application-aware dla wszystkich wspieranych wirtualizatorów.
2. System musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowanie zaawansowanych metod transportu (HotAdd, SAN, LAN), w tym metodami LAN-Free, tj. takimi, które podczas wykonywania backupu nie obciążają interfejsów sieciowych maszyn wirtualnych.
3. System kopii zapasowej musi wykorzystywać mechanizmy Change Block Tracking oraz Replica Change Tracking dla wspieranych przez producenta platformach wirtualizacyjnych.
4. Rozwiązanie producenta musi być certyfikowane przez dostawcę platformy wirtualizacyjnej, tj. producent musi uczestniczyć w programie Technology Alliance Partner.
5. System kopii zapasowej 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 oraz Hyper-V niezależnie od rodzaju storage-u użytego do przechowywania kopii zapasowych.
6. Dla środowiska vSphere i Hyper-V rozwiązanie powinno umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).
7. System kopii zapasowej musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere.
8. System kopii zapasowej musi umożliwiać weryfikację odtwarzalności wirtualnych maszyn według własnego harmonogramu w dowolnym środowisku.

Aplikacje SaaS

1. Ochrona z tej samej konsoli dla Microsoft 365 minimum na poziomie, skrzynek pocztowych, onedrive, kontaktów, kalendarza.

2. Rozwiązanie musi umożliwiać przywracanie danych Microsoft 365: do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku .pst oraz do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji)
3. System musi umożliwiać granularne odtwarzanie danych, tj. pojedynczych plików z kopii obrazu dysku oraz pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365.
4. System musi umożliwiać zabezpieczanie środowisk Git, w tym GitHub, GitLab oraz Bitbucket wraz z metadanymi
5. System musi umożliwiać odtworzenie dowolnego środowiska Git w dowolnym innym środowisku Git, tzw. odtwarzanie crossowe.
6. System musi umożliwiać zabezpieczenie metadanych zebranych wokół repozytorium w ramach zabezpieczanego środowiska Git.
7. System musi umożliwiać odtwarzanie metadanych repozytorium Git do dowolnego innego środowiska Git w przypadku chęci odtworzenia repozytorium.
8. System musi umożliwiać zabezpieczenie środowisk Jira
9. System musi umożliwiać odtworzenie środowiska Jira do chmury lub środowiska lokalnego.
10. System musi umożliwiać zabezpieczenie środowisk Jira

Licencjonowanie i wsparcie techniczne

1. Wszystkie linie supportu muszą być obsługiwane w języku polskim.
2. Wsparcie techniczne musi być świadczone bezpośrednio przez główną siedzibę producenta.
3. Możliwość zgłaszania ticketów supportowych bezpośrednio z poziomu interfejsu zarządzania w formie czatu.
4. Producent wraz z rozwiązaniem musi udostępnić materiały samopomocowe w j. polskim (minimum dostęp do bazy wiedzy, materiałów wideo oraz kart produktów)
5. Wsparcie techniczne musi umożliwiać korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego.
6. Licencje w ramach rozwiązania powinny pozwalać na zabezpieczenie określonej przez Zamawiającego ilości hostów w obrębie wspieranych przez System środowisk.
7. Licencje powinny być dostępne w opcji wieczystej .
8. Dostęp do wsparcia technicznego producenta powinno obowiązywać przez okres min. **12** miesięcy
9. Sposób licencjonowania opiera się na:
    - ilości serwerów/endpointów - dla fizycznych urządzeń,
    - ilości socketów w hostach - dla środowisk wirtualnych,
    - ilość repozytoriów - dla GIT.
10. Licencje powinny umożliwiać zabezpieczenie w wersji **wieczystej**:
    - 1 endpointa
    - 1 serwera

Anty-ransomware i bezpieczeństwo

1. System plików rozwiązania musi być odporny na ataki Ransomware (zapewnić ochronę przed szyfrowaniem end-to-end, kopie zapasowe nie mogą być nadpisywane - "niezmienny system plików").
2. System powinien umożliwiać wykorzystanie wbudowanego menedżera haseł do przechowywania wszelkich sekretów (haseł, danych dostępowych, kluczy szyfrujących) wykorzystywanych przez System
3. System powinien umożliwiać przywrócenie hasła głównego administratora w przypadku jego utraty.
4. W ramach systemu, komunikacja pomiędzy hostem źródłowym, a magazynem powinna odbywać się tylko i wyłącznie bezpośrednio pomiędzy agentem backupu, a magazynem. Komunikacja nie może przechodzić przez serwer backupu, ani żaden inny komponent, którego awaria sparaliżowały by działanie Systemu. System nie może posiadać pojedynczego punktu awarii.
5. System musi działać w zgodzie z regułą Zero-knowledge Encryption. Oznacza to, że wszelkie sekrety muszą być przechowywane w centralnym Managerze Haseł w postaci zaszyfrowanej algorytmem AES i być udostępniane agentowi dopiero w momencie rozpoczęcia wykonywania kopii zapasowej. Sekrety nie mogą być przechowywane w konfiguracji agenta na zabezpieczonym urządzeniu.

Zamawiający wymaga, aby całość dostarczanego sprzętu informatycznego była nowa i nieużywana. Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez Wykonawcę i wyłącznie w celu weryfikacji poprawności działania oraz instalacji niezbędnego, wymienionego w opisie przedmiotu zamówienia i SWZ oprogramowania.

<u>Równoważność:</u>

1. Zamawiający informuje, że w przypadku gdy określił w opisie wymagania z użyciem znaków towarowych, patentów, pochodzenia, norm, aprobat, specyfikacji technicznych lub systemów odniesienia, to należy traktować takie określenie jako przykładowe, które określa minimalne

oczekiwane parametry jakościowe oraz wymagany standard. W każdym takim przypadku Zamawiający dopuszcza zaoferowanie rozwiązań równoważnych.

2. Za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega znacząco od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym.
3. Wykonawca jest zobowiązany zastosować składowe o parametrach technicznych i jakościowych takich samych lub lepszych niż opisane, a zastosowanie ich w żaden sposób nie może wpłynąć negatywnie na prawidłowe funkcjonowanie urządzenia oraz wartość użytkową.

Kryteria równoważności:

1. **Minimalne wymagania dla oprogramowania równoważnego Windows Server 2022 Standard,16CORE**

System operacyjny musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1) możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek;
2) możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu;
3) wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6;
4) możliwość uruchomienia kontrolera domeny będącego w pełni zgodnym z domeną AD pracującą w oparciu o minimum system Windows Server* 2022 (poziom funkcjonalności AD DS Windows Server* 2022);
5) umożliwiającym upgrade i downgrade do dowolnej wspieranej przez producenta wersji oprogramowania,
6) możliwość uruchomienia kontrolera domeny tylko do odczytu;
7) możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny;
8) możliwość uruchomienia serwera usług terminalowych (RemoteApp) zgodnego z min. Windows Server* 2022;
9) obsługa zdalnego pulpitu;
10) możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;
11) obsługa PowerShell;
12) obsługa certyfikatów w AD;
13) obsługa drzewa katalogowego Active Directory;
14) zasady licencjonowania powinny pozwalać na instalację nieograniczonej liczby maszyn wirtualnych;
15) możliwość instalacji w środowisku wirtualizacyjnym VMWare ESX* w wersji 6.7 U3 lub nowszej;
16) wsparcie dla architektury 64 bitowej;
17) możliwość instalowania i uruchamiania oprogramowania oraz systemów posiadanych przez zamawiającego.

W przypadku zaoferowania oprogramowania równoważnego względem wyspecyfikowanego przez Zamawiającego w SWZ, Wykonawca musi na swój koszt przedstawić, że zaoferowane produkty spełniają wszystkie wymagania i warunki określone w SWZ, w szczególności w zakresie:

1) warunków licencji / sublicencji / subskrypcji zaoferowanych produktów równoważnych w każdym aspekcie, które nie mogą być gorsze niż dla produktów wymienionych w SWZ,

2) funkcjonalności zaoferowanych produktów równoważnych, które nie mogą być ograniczone i gorsze względem funkcjonalności produktów wymienionych w SWZ,
3) zakresu kompatybilności i współdziałania zaoferowanych produktów równoważnych ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego, który nie może być gorszy niż dla produktów wymienionych w SWZ,
4) poziomu zakłóceń pracy środowiska systemowo-programowego Zamawiającego spowodowanego wykorzystaniem zaoferowanych produktów równoważnych, który nie może być większy niż w przypadku produktów wymienionych w SWZ;
5) poziomu współpracy zaoferowanych produktów równoważnych z systemami Zamawiającego, który nie może być gorszy od tego jaki zapewniają produkty wymienione w SWZ,
6) zapewnienia pełnej, równoległej współpracy w czasie rzeczywistym i pełnej funkcjonalnej zamienności zaoferowanych produktów równoważnych z produktami wymienionymi w SWZ,
7) warunków i zakresu usług gwarancji, asysty technicznej i konserwacji zaoferowanych produktów równoważnych, które nie mogą być gorsze niż dla produktów wymienionych w SWZ,
8) obsługi przez zaoferowane produkty równoważne języków interfejsu, w ilości i rodzaju nie mniejszych niż oferują produkty wymienione w SWZ,
9) wymagań sprzętowych dla zaoferowanych produktów równoważnych, które nie mogą być wyższe niż dla produktów wymienionych w SWZ,
10) dostępności wersji na różne systemy operacyjne zaoferowanych produktów równoważnych, która nie może być mniejsza niż dla produktów wymienionych w SWZ.
11) W przypadku zaoferowania przez Wykonawcę produktu równoważnego Wykonawca dokona wspólnie z Zamawiającym instalacji i testowania produktu równoważnego w środowisku sprzętowo-programowym Zamawiającego.
12) W przypadku zaoferowania przez Wykonawcę oprogramowania równoważnego Wykonawca dokona transferu wiedzy w zakresie utrzymania i rozwoju rozwiązania opartego o zaproponowane produkty.
13) W przypadku, gdy zaoferowany przez Wykonawcę produkt równoważny nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po usunięciu produktu równoważnego.
14) Oprogramowanie równoważne dostarczane przez Wykonawcę nie może powodować utraty kompatybilności oraz wsparcia producentów innego używanego i współpracującego z nim oprogramowania.
15) Oprogramowanie równoważne zastosowane przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie oprogramowania równoważnego, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat licząc od momentu złożenia oferty. Niedopuszczalne jest użycie oprogramowania równoważnego, dla którego producent oprogramowania współpracującego ogłosił zaprzestanie wsparcia w jego nowszych wersjach.

2. **Minimalne wymagania dla licencji równoważnych 3 x 10-pack of Windows Server 2022/2019 User CALs , 10 x Microsoft SQL Server 2022 Standard, USER CALs , 1 x Microsoft SQL Server 2022 Standard**
   a) licencje równoważne muszą być kompatybilne i w sposób niezakłócony współdziałać z oprogramowaniem Microsoft SQL Server funkcjonującym u Zamawiającego;
   b) licencje równoważne nie mogą zakłócić pracy środowiska systemowo - programowego Zamawiającego;
   c) licencje równoważne muszą w pełni współpracować z systemami Zamawiającego, opartymi o dotychczas użytkowane oprogramowanie Microsoft Windows Server, Microsoft SQL Server 2019 Standard oraz Microsoft SQL Server 2022 Standard
   d) licencje równoważne muszą zapewniać pełną, równoległą współpracę w czasie rzeczywistym i pełną funkcjonalną zamienność oprogramowania równoważnego z wyspecyfikowanym oprogramowaniem.