Załącznik nr 1 do zapytania ofertowego

Opis przedmiotu zamówienia

Usługa dostawy, instalacji, konfiguracji i uruchomienia infrastruktury serwerowej

w Gminnym Przedsiębiorstwie Wodociągowym Sp. z o.o.

Odniesienia do znaków towarowych i rozwiązań producenta opisujące zamawiany przedmiot, a nie identyfikujące wyłącznie posiadane środowisko, odczytuje się ze słowami „lub równoważne". Równoważność oznacza spełnienie wymagań funkcjonalnych i wydajnościowych OPZ, zgodność z ujawnionym środowiskiem i interfejsami, zapewnienie wysokiej dostępności (HA) usług poprzez automatyczne przełączenie ich na drugi serwer w przypadku awarii pierwszego oraz zapewnienie wymaganych okresów wsparcia i praw licencyjnych. Rozwiązanie równoważne nie może wymagać dodatkowych zakupów po stronie Zamawiającego poza zasobami wyraźnie wskazanymi w OPZ. Wykonawca wskazuje takie rozwiązanie w ofercie i przedstawia porównanie oraz dowody spełnienia wymagań. Inna konstrukcja wewnętrzna lub nazwa handlowa nie stanowi podstawy odmowy równoważności, jeżeli wymagane rezultaty są zachowane.

1. **Serwer: 2 szt.**
   (wymagane jest dostarczenie dwóch takich samych serwerów, tego samego producenta)

OPIS WYMAGAŃ:

1	**Stan urządzenia**	Serwer używany, poddany profesjonalnej kontroli technicznej i przygotowaniu do ponownej eksploatacji (refurbished), kompletny, sprawny i przetestowany. Dopuszczalne normalne ślady użytkowania nieograniczające funkcjonalności. Urządzenie pozbawione blokad administracyjnych oraz przypisania do kont poprzednich użytkowników.
2	**Obudowa**	Obudowa przystosowana do montażu w szafie rack 19", o wysokości nie większej niż 2U. Minimum 8 wnęk na dyski 3,5" z możliwością montażu nośników 2,5" przy użyciu odpowiednich kieszeni lub adapterów. Dostęp serwisowy do dysków od frontu obudowy.
3	**Płyta główna**	Płyta główna serwerowa umożliwiająca jednoczesną pracę dwóch procesorów, obsługująca pamięć ECC RDIMM i minimum 16 gniazd pamięci RAM. Rozwiązanie zgodne z dostarczoną konfiguracją.

4	**Chipset**	Chipset klasy serwerowej, zgodny z zastosowanymi procesorami i obsługujący pracę dwuprocesorową.
5	**Procesor**	Zainstalowane 2 procesory klasy serwerowej x86-64, każdy z minimum 22 fizycznymi rdzeniami i 44 wątkami, taktowanie bazowe nie niższe niż 2,10 GHz. Łącznie minimum 44 rdzenie fizyczne i 88 wątków na serwer.
6	**Pamięć RAM**	Minimum 256 GB pamięci operacyjnej DDR4 ECC RDIMM, zainstalowanej w 16 modułach po 16 GB, o szybkości co najmniej 2666 MT/s. Moduły sprawne i zgodne z płytą główną.
7	**Kontroler RAID**	Dedykowany sprzętowy kontroler macierzowy SAS/SATA, wyposażony w pamięć podręczną zabezpieczoną przed utratą danych, obsługujący co najmniej RAID 0, 1, 5, 6 i 10. Kontroler zgodny z zastosowaną płytą główną i dostarczonymi dyskami.
8	**Dyski twarde**	Zainstalowane minimum 2 nośniki SSD SATA o pojemności nie mniejszej niż 480 GB każdy, w formacie 2,5", klasy przeznaczonej do pracy serwerowej, wraz z odpowiednimi kieszeniami lub adapterami. Nośniki sprawne, bez krytycznych błędów SMART. Wymagana możliwość skonfigurowania RAID 1.
9	**Gniazda rozszerzeń**	Serwer wyposażony w złącza rozszerzeń PCI Express umożliwiające instalację dodatkowych kart. Wszystkie podzespoły zamontowane w sposób zapewniający prawidłową pracę i chłodzenie.
10	**Interfejsy sieciowe**	Minimum 2 porty sieciowe obsługujące szybkości 10/25 Gb/s w standardzie SFP28, zapewnione przez wewnętrzną kartę sieciową montowaną w dedykowanym złączu serwerowym. Wymagane sprawne porty i sterowniki umożliwiające eksploatację. Moduły optyczne i przewody połączeniowe nie są objęte dostawą, o ile nie wskazano inaczej.
11	**Wbudowane porty**	Wymagane porty umożliwiające lokalną administrację, w szczególności USB oraz wyjście wideo; dedykowany port sieciowy do zdalnego zarządzania serwerem.
12	**Grafika**	Zintegrowany układ graficzny umożliwiający lokalną obsługę konsoli serwera.

13	**Zasilacze**	Dwa zasilacze serwerowe pracujące redundantnie, przystosowane do wymiany serwisowej i odpowiednie do konfiguracji sprzętowej. Dołączone przewody zasilające.
14	**Elementy montażowe**	Komplet kompatybilnych szyn do montażu każdego serwera w szafie rack 19".
15	**System operacyjny**	Dla każdego z dwóch dostarczanych serwerów wymagane jest dostarczenie licencji na system operacyjny Windows Server 2025 Standard w modelu licencjonowania opartym na fizycznych rdzeniach procesorów, z prawem do użytkowania na oferowanym serwerze. Licencje muszą obejmować wszystkie 44 rdzenie fizyczne każdego serwera (2 procesory po 22 rdzenie), tj. na jeden serwer: jeden pakiet licencyjny obejmujący 16 rdzeni oraz 14 pakietów uzupełniających po 2 rdzenie. Łącznie dla dwóch serwerów: 2 pakiety 16-rdzeniowe oraz 28 pakietów 2-rdzeniowych (88 licencjonowanych rdzeni). Licencje muszą być oryginalne, legalne, przeznaczone do oferowanego sprzętu i umożliwiać aktywację systemu. Dostawa obejmuje niezbędne klucze aktywacyjne oraz dokumentację potwierdzającą uprawnienie do korzystania z systemu. Wymagana edycja Standard, wersja 2025, 64-bit.
16	**Bezpieczeństwo**	Możliwość zabezpieczenia dostępu do ustawień BIOS/UEFI hasłem. Mechanizmy zabezpieczenia uruchamiania dostępne w oferowanej platformie. Przed dostawą należy usunąć dane poprzedniego użytkownika i przywrócić bezpieczną konfigurację administracyjną. Moduł TPM wymagany wyłącznie, jeżeli jest fizycznie zainstalowany i wyszczególniony przez wykonawcę w ofercie.
17	**Karta zarządzania**	Zintegrowany kontroler zdalnego zarządzania w rozszerzonej, aktywnej wersji licencyjnej, działający niezależnie od systemu operacyjnego. Minimum: dostęp do panelu WWW, zdalny odczyt stanu sprzętu, dziennik zdarzeń, zdalne włączanie i wyłączanie, konsola KVM przez sieć, możliwość montowania zdalnych nośników oraz konfiguracja parametrów sieciowych karty. Wymagane przekazanie uprawnień administratora do urządzenia.
18	**Oprogramowanie do zarządzania**	Możliwość zarządzania i monitorowania stanu sprzętu przy użyciu wbudowanej karty zarządzania oraz narzędzi zgodnych z oferowanym serwerem. Nie wymaga się dodatkowych płatnych licencji na platformę centralnego zarządzania.

19	**Oprogramowanie do monitorowania**	Dostęp do podstawowych informacji diagnostycznych i eksploatacyjnych, w tym stanu procesorów, pamięci RAM, dysków, zasilaczy i czujników temperatury, za pośrednictwem wbudowanych funkcji zarządzania. Nie wymaga się usługi monitorowania w chmurze ani funkcji predykcyjnych.
20	**Certyfikaty i zgodność**	Sprzęt fabrycznie przeznaczony do zastosowań serwerowych i posiadający oznakowanie zgodności wymagane przy pierwotnym wprowadzeniu na rynek UE. Dopuszczone urządzenia refurbished; nie wymaga się aktualnych certyfikatów środowiskowych przypisanych wyłącznie do nowych modeli.
21	**Dokumentacja i odbiór**	Dokumentacja techniczna w języku polskim lub angielskim, dopuszczalna w postaci elektronicznej. Przy dostawie należy podać numery seryjne, specyfikację faktycznie zainstalowanych podzespołów oraz potwierdzić przeprowadzenie testów sprawności. Serwery muszą uruchamiać się bez błędów sprzętowych uniemożliwiających eksploatację.
22	**Warunki gwarancji**	Minimum 36 miesięcy gwarancji udzielanej przez sprzedawcę lub wykonawcę, liczonej od dnia odbioru. Obsługa zgłoszeń serwisowych z reakcją NBD, tj. najpóźniej w następnym dniu roboczym po przyjęciu prawidłowego zgłoszenia. W ramach gwarancji wykonawca zapewnia diagnostykę, naprawę lub wymianę wadliwych podzespołów na zgodne i sprawne. Koszt części oraz realizacji świadczeń gwarancyjnych ponosi wykonawca. Wsparcie producenta urządzenia nie jest warunkiem obowiązywania gwarancji sprzedawcy.

2. Napęd Streamer i/lub kasety do Streamer'a: 1 szt.

OPIS WYMAGAŃ:

1	**Wymagania ogólne**	Autoloader/biblioteka taśmowa w obudowie RACK • Typ napędu zainstalowanego napędu – LTO 8 z interfejsem SAS • Liczba zainstalowanych napędów – 1 szt. • Liczba obsługiwanych napędów - 1 szt. • Liczba dostarczonych aktywnych slotów – 9 szt. • Wbudowany skaner kodów paskowych na nośnikach LTO • Lokalne zarządzanie za pomocą panelu/pulpitu operatora • Obsługa szyfrowania danych na nośniku LTO • Wsparcie SSL • Gwarantowana kompatybilność odczytu taśm LTO-7 • Gwarantowana kompatybilność zapisu taśm LTO-7 • Interfejs zdalnego zarządzania - Ethernet 10/100Mb/s złącze RJ-45 • 10 nośników LTO-8
2	**Gwarancja jakości producenta:**	Wykonawca zapewni gwarancję producenta typu Onsite NBD, obejmującą świadczenie usług serwisowych w miejscu instalacji urządzenia, z czasem reakcji serwisu nie dłuższym niż następny dzień roboczy od skutecznego zgłoszenia awarii. Gwarancja obejmuje diagnostykę, robociznę, części zamienne oraz ich wymianę bez dodatkowych kosztów dla Zamawiającego.

3. Macierz: 1 szt.

OPIS WYMAGAŃ:

1	**Stan urządzenia**	Urządzenie odnowione (refurbished), używane, sprawne technicznie, przetestowane przed dostawą. Wszystkie dostarczone komponenty muszą być kompatybilne i umożliwiać prawidłową pracę urządzenia.
2	**Typ obudowy**	Obudowa do montażu w szafie rack 19”, o wysokości maksymalnie 3U; minimum 30 wnęk na dyski 2,5”.
3	**Przestrzeń dyskowa**	Zainstalowane minimum 8 dysków twardych SAS 2,5”, każdy o pojemności minimum 1,8 TB i prędkości obrotowej minimum 10 000 obr./min; dyski przystosowane do pracy w macierzach dyskowych. Łączna pojemność surowa zainstalowanych dysków: minimum 14,4 TB.
4	**Obsługa dysków i rozbudowa**	Obsługa dysków w wymiennych kieszeniach oraz możliwość rozbudowy pojemności przez instalację kolejnych dysków w wolnych zatokach obudowy, bez wymiany całej macierzy.
5	**Sposób zabezpieczenia danych**	Obsługa redundantnej organizacji grup dyskowych z ochroną danych przy awarii dysku, w szczególności poziomów RAID 5 i RAID 6 lub funkcjonalnie równoważnego mechanizmu ochrony danych. Możliwość tworzenia i udostępniania wolumenów logicznych (LUN).
6	**Tryb pracy kontrolerów macierzowych**	Minimum 2 niezależne kontrolery macierzowe zapewniające wysoką dostępność i redundancję dostępu do danych. Awaria pojedynczego kontrolera nie może powodować utraty dostępu do danych przy prawidłowo skonfigurowanych połączeniach hostów.
7	**Interfejsy komunikacyjne**	Co najmniej 8 portów Ethernet 10 Gb/s w standardzie SFP+ przeznaczonych do komunikacji blokowej iSCSI, po minimum 4 porty na każdy kontroler.
8	**Protokoły dostępu**	Obsługa blokowego udostępniania zasobów przez protokół iSCSI w sieci Ethernet 10 Gb/s.
9	**Zarządzanie**	Możliwość konfiguracji i zarządzania macierzą z poziomu interfejsu administracyjnego, w tym zarządzania dyskami, pulami dyskowymi, wolumenami logicznymi oraz mapowaniem zasobów do serwerów.
10	**Zarządzanie wolumenami**	Możliwość tworzenia wielu wolumenów logicznych i ich prezentowania serwerom poprzez iSCSI; możliwość nadawania uprawnień dostępu do wolumenów dla wskazanych hostów.
11	**Obsługa wielu ścieżek**	Możliwość podłączenia serwerów z wykorzystaniem redundantnych ścieżek dostępu (multipathing) w celu zapewnienia ciągłości pracy w przypadku awarii pojedynczego połączenia lub kontrolera.
12	**Redundancja**	Macierz musi być wyposażona w dwa kontrolery oraz dwa redundantne zasilacze. Dyski muszą być wymienne bez konieczności demontażu macierzy z szafy rack.
13	**Zasilanie**	Dwa zasilacze przystosowane do zasilania z sieci 230 V AC, umożliwiające redundancję zasilania.

14	**Elementy montażowe**	Komplet szyn do montażu urządzenia w standardowej szafie rack 19”.
15	**Licencje i funkcjonalność**	Urządzenie należy dostarczyć z aktywnymi i zgodnymi z warunkami licencyjnymi uprawnieniami niezbędnymi do uruchomienia oraz eksploatacji zaoferowanej konfiguracji, w tym do udostępniania zasobów blokowych przez iSCSI. Funkcje dodatkowo licencjonowane nie są wymagane, o ile nie wskazano ich wprost w niniejszym OPZ.
16	**Dokumentacja**	Dokumentacja pozwalająca na uruchomienie, konfigurację i podstawową administrację urządzeniem, w języku polskim lub angielskim.
17	**Warunki dostawy**	Urządzenie kompletne, wyposażone w opisane kontrolery, dyski, zasilacze i szyny montażowe. Przed dostawą wykonawca powinien zweryfikować sprawność dysków, kontrolerów, zasilaczy oraz portów komunikacyjnych.
18	**Warunki gwarancji**	Minimum 36 miesięcy gwarancji udzielanej przez sprzedawcę, licząc od dnia dostawy. Serwis w standardzie NBD (Next Business Day): podjęcie obsługi zgłoszenia i zapewnienie interwencji serwisowej w następnym dniu roboczym, zgodnie z warunkami gwarancji. W okresie gwarancji wykonawca zapewnia diagnostykę oraz naprawę albo wymianę uszkodzonych elementów bez dodatkowych kosztów dla zamawiającego.
19	**Stan urządzenia**	Urządzenie odnowione (refurbished), używane, sprawne technicznie, przetestowane przed dostawą. Wszystkie dostarczone komponenty muszą być kompatybilne i umożliwiać prawidłową pracę urządzenia.
20	**Typ obudowy**	Obudowa do montażu w szafie rack 19”, o wysokości maksymalnie 3U; minimum 30 wnęk na dyski 2,5”.
21	**Przestrzeń dyskowa**	Zainstalowane minimum 8 dysków twardych SAS 2,5”, każdy o pojemności minimum 1,8 TB i prędkości obrotowej minimum 10 000 obr./min; dyski przystosowane do pracy w macierzach dyskowych. Łączna pojemność surowa zainstalowanych dysków: minimum 14,4 TB.

4. System Backupowy: obsługa do 5 maszyn Wirtualnych z bezpłatną aktualizacja na 3 lata.

OPIS WYMAGAŃ:

1	**Wymagania ogólne**	• 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 Peer Insights: i spełniać minimalne wymaganie : - minimalna liczba referencji 500, - minimalna ocena z referencji 4,6. • Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 7.x do 9.1 oraz Microsoft Hyper-V 2016 do 2025. Wszystkie funkcjonalności w specyfikacji muszą być dostępne dla powyższych platform wirtualizacyjnych, chyba, że wyszczególniono inaczej • Oprogramowanie musi współpracować z infrastrukturą Nutanix w wersji 6.8.x lub nowsze, Red Hat Virtualization 4.5, Oracle Linux Virtualization 4.5 lub nowszy, Proxmox VE 8.2 do 9.2, Scale Computing HyperCore 9.4.32.218226 – 9.6.x, Citrix XenServer 8.4 lub nowszy, XCP-ng 8.3 lub nowszy, HPE Morpheus 8.0.13-2 do 9.0 • 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, Microsoft Azure Data Lake, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
2	**Całkowite koszty posiadania**	• System backupowy musi mieć możliwość wdrożenia wszystkich komponentów (np. serwer backupowy, serwer pośredniczący, repozytorium) na platformach Windows oraz Linux • System backupowy musi mieć mieć możliwość wdrożenia w oparciu o tzw. appliance zgodny z wytycznymi bezpieczeństwa DISA (Defense Information Systems Agency) • 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 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 wiele wirtualnych puli pamięci na kopie zapasowe. Wymagane jest wsparcie dla co najmniej 20 pamięci masowych w pojedyńczej puli. • Oprogramowanie musi umożliwiać ochronę kopii zapasowych generowanych przez dowolną aplikację posiadającą możliwość zapisu danych na udział NFS, z zapewnieniem mechanizmów snapshotów, niezmienności danych, retencji, szybkiego przywracania oraz kopiowania danych do dodatkowych lokalizacji archiwizacyjnych. • Oprogramowanie musi pozwalać na przechowywanie kopii bezpieczeństwa w chmurze producenta. • Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage, IBM Cloud Storage, 11:11 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 do backupu oraz odtwarzania obrazu maszyny wirtualnej • 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 umożliwiać tworzenie logicznie odseparowanych środowisk dla różnych organizacji/działów. Dodatkowo system musi wspierać kontrolę dostępu w oparciu o role (RBAC) - predefiniowane lub własne • 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 natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej

		• Oprogramowanie musi umożliwiać integracje z różnymi dostarczycielami tożsamości (IdP - Identity Providers) z wykorzystaniem protokołu SAML (np. Entra ID, Okta) • Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora, reset zablokowanego konta) • Oprogramowanie musi posiadać integracje z systemami zarządania kluczami szyfrującymi (KMS) • Oprogramowanie musi posiadać integracje z systemami typu SIEM • Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej oraz analizy istniejącej instalacji systemu backupowego. Powinna istnieć możliwość wyłączenia tej opcji. • Oprogramowanie musi pozwalać na wydawanie komend głosowych asystentowi AI
3	**Wymagania RPO**	• 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 conajmniej dla platformy VMware i Hyper-V • 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 - 2025 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, pomiędzy hostami Hyper-V oraz pomiędzy hostami Proxmox VE. • Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, systemu operacyjnego Windows Server lub Linux (z innych platfrom - fizycznych, wirtualnych, chmurowych). 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)
4	**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, Nutanix AHV oraz Proxmox VE niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. • Dodatkowo dla środowiska vSphere, Hyper-V, Nutanix AHV, Proxmox VE i MS Azure 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 platformę. 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, zarówno fizycznej jak i wirtualnej • Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i 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 wspierać bezagentowy backup, spójny aplikacyjnie (tzw. Application Consistent) dla maszyn wirtualnych z platfrom vSphere, Hyper-V, Nutanix AHV, Proxmox. • Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej (Minimum dla Active Directory, MS Exchange, MS SQL, MS Sharepoint, Oracle i PostgreSQL). • Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects oraz pozwalać na odtworzenie haseł. • Oprogramowanie musi pozwalać na backup i odtwarzanie usługi Entra ID. W szczególności użytkowników, grupy, role, jednostki administracyjne, entrprise applications, Conditional Access Policies, Intune Policies oraz logi audytowe i sign-in. • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange (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. 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. 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 MongoDB. 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 •
5	**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 • 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 posiadać swój wbudowany program antywirusowy zoptymalizowany do przeszukiwania kopii backupowych • 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 wyuczonynym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków • Oprogramowanie musi posiadać mechanizm wykrywania oznak ataku hakerskiego tzw Indicators of Compromise • Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. • Oprogramowanie musi mieć możliwość integracji z innymi systemami bezpieczeństwa - minimum Splunk, Palo Alto Networks XSOAR/XSIAM, CrowdStrike Falcon LogScale, Microsoft Sentinel.
6	**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, Oracle Linux, SLES, Rocky Linux, AlmaLinux • 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 oraz odzyskiwanie 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 deduplikacje 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, Microsoft Active Directory, Microsoft Sharepoint, Microsoft SQL, Oracle, PostgreSQL oraz MongoDB • 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

7	**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 7.x – 9.0 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 2016 – 2025 oraz Azure Stack HCI 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
8	**Raportowanie**	• System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 7.x – 9.0 – 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 2016 – 2025 oraz Azure Stack HCI 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, 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 • System musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej oraz analizy istniejącej instalacji systemu backupowego. Powinna istnieć możliwość wyłączenia tej opcji.

5. Wdrożenie urządzeń, oprogramowania do wykonywania kopii zapasowych, w tym deduplikacji - rozwiązań z zakresu bezpieczeństwa
Oprogramowanie do wykonywania kopii zapasowych, w tym deduplikacji: 1 szt.

OPIS WYMAGAŃ:

1	**Infrastruktura objęta usługą**	• Serwery fizyczne 2 szt. (instalacja, konfiguracja i uruchomienie klastra HA) • Macierz dyskowa (konfiguracja przestrzeni dyskowej, redundancji i połączeń) • Urządzenie LTO (konfiguracja i integracja z systemem backupu) • Oprogramowanie wirtualizacyjne HyperV (instalacja i konfiguracja klastra) • Backup & Replication Instalacja (konfiguracja i uruchomienie systemu backupu) • Repozytorium kopii zapasowych (konfiguracja, zabezpieczenie i integracja)
2	**Zakres prac – instalacja i konfiguracja serwerów**	• Konfiguracji kontrolerów dyskowych i nośników przeznaczonych na systemy operacyjne. • Instalacji i konfiguracji oprogramowania wirtualizacyjnego Hyper-V • Konfiguracji interfejsów sieciowych oraz połączeń z macierzą dyskową. • Konfiguracji sieci zarządzającej, produkcyjnej, migracyjnej i komunikacji z systemem backupu wraz ze zespołem z ramienia zamawiającego • Konfiguracji synchronizacji czasu i usług zarządzania. • Zabezpieczenia interfejsów administracyjnych i konfiguracji dostępu administratorów. • Weryfikacji poprawności działania wszystkich interfejsów oraz połączeń. wraz ze zespołem z ramienia zamawiającego
3	**Konfiguracja klastra wysokiej dostępności (HA)**	Zakres prac obejmuje: • Utworzenie klastra wirtualizacyjnego. • Dodanie obu serwerów do klastra. • Konfigurację współdzielonej przestrzeni dyskowej. • Konfigurację mechanizmów monitorowania dostępności węzłów. • Konfigurację quorum/witness, zgodnie z wymaganiami zastosowanej platformy. • Konfigurację automatycznego ponownego uruchamiania maszyn wirtualnych na dostępnym serwerze po awarii drugiego. • Konfigurację priorytetów uruchamiania maszyn wirtualnych.

		• Konfigurację migracji maszyn wirtualnych pomiędzy serwerami, jeżeli wspiera ją wykorzystywana platforma. • Konfigurację mechanizmów zapobiegania zjawisku split-brain. • Przeprowadzenie testów awaryjnego przełączenia i ponownego uruchomienia usług. Wymagany rezultat: prawidłowo skonfigurowany klaster umożliwiający automatyczne wznowienie działania objętych nim maszyn wirtualnych na sprawnym serwerze w przypadku awarii drugiego węzła, w granicach dostępnych zasobów i możliwości technicznych platformy.
4	**Konfiguracja macierzy dyskowej**	• Weryfikację stanu technicznego macierzy oraz dostępnych zasobów. • Konfigurację grup dyskowych i poziomów RAID. • Utworzenie wymaganych wolumenów logicznych. • Konfigurację udostępniania zasobów dyskowych obu serwerom. • Konfigurację redundantnych ścieżek dostępu (MPIO/multipathing), o ile wspiera je infrastruktura. • Konfigurację uprawnień dostępu do wolumenów. • Konfigurację mechanizmów monitorowania stanu macierzy. • Konfigurację powiadomień o awariach dysków i kontrolerów. • Przeprowadzenie testów dostępności przestrzeni dyskowej z obu węzłów klastra
5	**Instalacja i konfiguracja Backup & Replication**	Wykonawca zobowiązany będzie do instalacji i konfiguracji systemu Backup & Replication w środowisku Zamawiającego. • Przygotowanie środowiska systemowego dla Backup & Replication. • Instalację oprogramowania. • Konfigurację podstawowych usług i komponentów. • Integrację z wykorzystywaną platformą wirtualizacyjną. • Konfigurację dostępu do chronionych zasobów. • Konfigurację kont i uprawnień administracyjnych. • Konfigurację powiadomień o stanie systemu • zadania wykonywania pełnych i przyrostowych kopii zapasowych; • harmonogramy backupu;

		• deduplikację danych; • kompresję danych; • szyfrowanie kopii zapasowych; • polityki retencji; • weryfikację poprawności wykonanych kopii; • raportowanie wyników zadań; • powiadomienia o błędach i niepowodzeniach;kopie konfiguracji systemu archiwizacjionfiguracji repozytorium na zasobach wskazanych przez Zamawiającego. • Konfiguracji dostępu do repozytorium. • Zastosowania mechanizmów ograniczających możliwość nieuprawnionego usunięcia lub modyfikacji kopii. • Konfiguracji mechanizmu niezmienialności kopii (immutability), jeżeli udostępniona infrastruktura spełnia wymagania techniczne. • Konfiguracji zasad wykorzystania przestrzeni dyskowej. • Weryfikacji wydajności zapisu i odczytu kopii zapasowych. Repozytorium kopii zapasowych powinno być odseparowane od produkcyjnych zasobów dyskowych w stopniu możliwym do uzyskania przy wykorzystaniu infrastruktury Zamawiającego. Harmonogramy i polityki retencji zostaną uzgodnione z Zamawiającym przed uruchomieniem produkcyjnym Zakres prac obejmuje: 1. Weryfikację poprawności podłączenia urządzenia LTO. 2. Konfigurację sterowników i interfejsów komunikacyjnych. 3. Integrację urządzenia z systemem Backup & Replication. 4. Konfigurację urządzenia w systemie backupowym. 5. Konfigurację zadań kopiowania danych na nośniki LTO. 6. Konfigurację zasad retencji kopii taśmowych. 7. Konfigurację katalogowania nośników. 8. Przygotowanie procedury wymiany i przechowywania taśm. 9. Przeprowadzenie testowego zapisu danych na nośniku.

		10. Przeprowadzenie testowego odtworzenia danych z nośnika LTO. •
6	**Konfiguracja i integracja urządzenia LTO**	• Weryfikację poprawności podłączenia urządzenia LTO. • Konfigurację sterowników i interfejsów komunikacyjnych. • Integrację urządzenia z systemem Backup & Replication. • Konfigurację urządzenia w systemie backupowym. • Konfigurację zadań kopiowania danych na nośniki LTO. • Konfigurację zasad retencji kopii taśmowych. • Konfigurację katalogowania nośników. • Przygotowanie procedury wymiany i przechowywania taśm. • Przeprowadzenie testowego zapisu danych na nośniku. • Przeprowadzenie testowego odtworzenia danych z nośnika LTO
7	**Konfiguracja zabezpieczeń środowiska**	• Ograniczenie dostępu do interfejsów administracyjnych. • Konfigurację indywidualnych kont administratorów. • Konfigurację mechanizmów uwierzytelniania wieloskładnikowego, w zakresie obsługiwanym przez oprogramowanie. • Segmentację ruchu sieciowego związanego z zarządzaniem i backupem wraz ze zespołem z ramienia zamawiające • Konfigurację szyfrowania transmisji i kopii zapasowych. • Konfigurację rejestrowania zdarzeń administracyjnych. • Konfigurację powiadomień o błędach i zdarzeniach bezpieczeństwa. • Weryfikację ustawień bezpieczeństwa oprogramowania i usług. • Ograniczenie możliwości usunięcia kopii zapasowych przez konta administrujące środowiskiem produkcyjnym. •
8	**Testy funkcjonalne i odbiorowe**	Wykonawca przeprowadzi co najmniej następujące testy: • Awaria pierwszego serwera (Uruchomienie objętych HA maszyn na drugim serwerze) • Awaria drugiego serwera (Uruchomienie objętych HA maszyn na pierwszym serwerze) • Dostęp do macierzy (Poprawna komunikacja obu serwerów)

		• Awaria jednej ścieżki dostępu do macierzy (Zachowanie dostępu do danych, jeżeli istnieją redundantne ścieżki) • Wykonanie pełnej kopii zapasowej (Poprawne zakończenie zadania) • Wykonanie kopii przyrostowej (Poprawne zakończenie zadania) • Odtworzenie pliku (Poprawne odtworzenie danych) • Odtworzenie maszyny wirtualnej (Poprawne uruchomienie odtworzonej maszyny) • Zapis danych na LTO (Poprawne zakończenie operacji) • Odtworzenie danych z LTO (Poprawne odtworzenie danych) • Test deduplikacji i kompresji (Potwierdzenie działania mechanizmów) • Test zabezpieczeń kopii (Potwierdzenie skonfigurowanych ograniczeń dostępu) • Test powiadomień (Prawidłowe dostarczenie komunikatów) • Test odtworzenia konfiguracji (Potwierdzenie możliwości odzyskania konfiguracji) •
9	**Dokumentacja powykonawcza**	Wykonawca przekaże Zamawiającemu dokumentację zawierającą co najmniej: • Opis architektury wdrożonego rozwiązania. • Schemat konfiguracji klastra HA. • Konfigurację serwerów i macierzy. • Opis konfiguracji sieci i połączeń. • Dokumentację systemu Backup & Replication. • Harmonogramy kopii zapasowych. • Politykę retencji. • Instrukcję odtwarzania maszyn wirtualnych i plików. • Instrukcję odtwarzania danych z LTO. • Procedurę postępowania w przypadku awarii serwera. • Procedurę postępowania w przypadku awarii systemu backupowego. • Wyniki testów odbiorowych.
10	**Szkolenie administratorów**	Wykonawca przeprowadzi instruktaż praktyczny dla administratorów Zamawiającego obejmujący: • zarządzanie klastrem HA; • monitorowanie stanu serwerów i macierzy; • obsługę Veeam Backup & Replication;

		• wykonywanie i kontrolowanie kopii zapasowych; • odtwarzanie plików i maszyn wirtualnych; • obsługę urządzenia LTO; • postępowanie w przypadku awarii.
11	**Wymagania dotyczące realizacji usługi**	• Wykonawca wykona prace z wykorzystaniem infrastruktury i licencji udostępnionych przez Zamawiającego. • Przed rozpoczęciem konfiguracji Wykonawca zweryfikuje kompatybilność poszczególnych elementów środowiska. • W przypadku stwierdzenia ograniczeń technicznych Wykonawca poinformuje Zamawiającego o ich wpływie na realizację wymagań. • Prace mogące powodować przerwy w dostępności usług wymagają wcześniejszego uzgodnienia z Zamawiającym. • Wykonawca nie może dokonywać operacji powodujących utratę danych bez uprzedniej zgody Zamawiającego. • Wykonawca zapewni odpowiednie zabezpieczenie kont i danych, do których uzyska dostęp. • Wykonawca przekaże Zamawiającemu wszystkie konfiguracje i informacje niezbędne do samodzielnej administracji środowiskiem. • Wykonawca ponosi odpowiedzialność za poprawność wykonanych prac konfiguracyjnych.
12	**Gwarancja na wykonane usługi**	• Wykonawca udzieli minimum 12-miesięcznej gwarancji na poprawność wykonanych prac instalacyjnych i konfiguracyjnych. • W okresie gwarancji Wykonawca zobowiązany będzie do nieodpłatnego usuwania błędów wynikających z nieprawidłowego wykonania usługi, w szczególności błędów konfiguracji klastra HA, macierzy, systemu backupu oraz urządzenia LTO. • Gwarancja nie obejmuje awarii sprzętowych ani wad oprogramowania niezwiązanych z działaniami Wykonawcy.

ZATWIERDZAM:

Tomasz Sikora

Prezes Zarządu

Gminnego Przedsiębiorstwa Wodociągowego

Sp. z o.o.

Signed by /
Podpisano przez:

Tomasz Marcin
Sikora

Date / Data: 2026-
11-10 12:21

(podpis kierownika Zamawiającego

lub osoby upoważnionej)