



Załącznik nr 3: Opis przedmiotu zamówienia

Część nr 1: Dostawa 2 szt serwerów typu NAS wraz z oprogramowaniem do wykonywania kopii zapasowych

Kompleksowe, zintegrowane rozwiązanie do backupu wraz z usługą wdrożenia w siedzibie Klienta oraz pomocą techniczną wykonawcy na okres 1 roku.

W zastosowanym rozwiązaniu oprogramowanie do centralnego zarządzania backupem ma być zintegrowane z platformą sprzętową serwera NAS tak aby nie było potrzeby instalacji serwera backupu (serwera zarządzania) na osobnym serwerze klienta.

System powinien umożliwić archiwizację nieograniczonej liczby punktów końcowych Windows, maszyn wirtualnych VMware, Hyper-V i serwerów plików. Bez dodatkowych kosztów licencji na oprogramowanie.

Zamawiający wymaga dostarczenia i wdrożenia rozwiązania składającego się z urządzenia NAS, dysków twardych oraz oprogramowania do backupu spełniających poniższe wymagania.

Minimalna specyfikacja platformy sprzętowej:

Procesor	Wielordzeniowy, zgodny z architekturą x86. Zaoferowany procesor musi uzyskiwać w teście Passmark CPU Mark wynik min.: 4.800 punktów na dzień 29.04.2025r. (wyniki procesorów załączone do SIWZ)
Obudowa	Rack 1U; komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.
Ilość obsługiwanych dysków	4 dysków 3,5" lub 2,5" SATA HDD/SSD z możliwością podłączenia półki rozszerzającej o 4 dyski
Pamięć RAM	16 GB pamięci SO-DIMM DDR4 z możliwością rozszerzenia do 32GB
Zainstalowane dyski	2 dyski HDD klasy Enterprise w formacie 3,5" znajdujących się na liście kompatybilności producenta macierzy NAS o min. pojemności 8TB; możliwość aktualizacji oprogramowania dysku z poziomu NAS; min. 2 mln MTBF
Interfejsy sieciowe	4 x Gigabit (10/100/1000); Wsparcie dla Link Agregation



Cyberbezpieczny Samorząd

Porty	2 x USB 3.2, 1 x eSATA, 1 x port konsoli
Wskaźniki LED	Zasilanie, alert, status, LAN, HDD1-4
Obsługa RAID	JBOD, RAID 0,1,5,6,10
Funkcje RAID	Możliwość zwiększania pojemności i migracja między poziomami RAID online.
Protokoły	SMB, AFP, NFS, FTP, WebDAV, Rsync, iSCSI, SSH, SNMP, VPN
Usługi	Serwer VPN, Serwer pocztowy, Stacja monitoringu, Windows ACL, Integracja z Windows ADS, Firewall, Serwer WWW, Serwer plików, Manager plików przez WWW, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Antywirus, Klient VPN, Usługa, Serwer i klient LDAP, Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID, prywatna chmura.
Obsługa migawek	TAK
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów
Język GUI	Polski
Gwarancja i serwis	5 lat gwarancji door-to-door producenta lub autoryzowanego partnera producenta na urządzenie i 5 lat gwarancji door-to-door producenta lub autoryzowanego partnera producenta na dyski. W przypadku wymiany uszkodzonego dysku na nowy, stary dysk pozostanie w rękach Zamawiającego.
System plików	Dyski wewnętrzne EXT4. Dyski zewnętrzne FAT, NTFS, EXT3, EXT4, HFS+
Liczba wolumenów	64
Liczba iSCSI Targetów	64
Liczba iSCSI LUN	128
Zasilanie	Redundantny, podwójny



Cyberbezpieczny Samorząd

Zintegrowane z serwerem NAS oprogramowanie do tworzenia kopii zapasowych musi spełniać następujące wymagania:

Konsola administratora

- Zintegrowane rozwiązanie do tworzenia kopii zapasowych dla serwerów fizycznych z systemem Windows i Linux, komputerów z systemem Windows i komputerów Mac, serwerów plików rsync i SMB oraz maszyn wirtualnych VMware vSphere i Microsoft Hyper-V
- Centralny interfejs zarządzania służący do monitorowania stanu wszystkich zadań tworzenia kopii zapasowych, zużycia pamięci masowej i transmisji danych historycznych
- Różne metody przywracania, w tym przywracanie całego urządzenia, natychmiastowe przywracanie, szczegółowe odzyskiwanie plików
- Elastyczne zasady planowania i przechowywania w celu dostosowywania strategii tworzenia kopii zapasowych
- Szczegółowe logi i raporty umożliwiające śledzenie stanów kopii zapasowych i diagnostykę problemów
- Możliwość jednoczesnego tworzenia kopii zapasowej 30 komputerów osobistych, serwerów fizycznych i maszyn wirtualnych.
- Możliwość szyfrowania kopii zapasowej
- Generowanie raportów według dostosowanego harmonogramu w celu śledzenia ogólnego stanu kopii zapasowej
 - Szczegółowe dzienniki i historia zadań dotyczące stanu kopii zapasowej urządzenia, anulowanych zadań, niepowodzeń tworzenia kopii zapasowej, migracji przywracania i przywracania urządzeń

Obsługa komputerów osobistych (Windows)

Dane techniczne

- Obsługiwane platformy: Windows 11 (wszystkie wersje), Windows 10 (wszystkie wersje), Windows 8.1 (wszystkie wersje)
- Obsługa systemu plików NTFS
- Tryby tworzenia kopii zapasowej: Kopia zapasowa całego urządzenia, wolumenu systemowego i niestandardowego wolumenu
- Metody przywracania: Przywracanie całego urządzenia, przywracanie na poziomie plików/folderów oraz przywracanie na poziomie woluminów
- Kopia zapasowa oparta na obrazie tworzy kopie zapasowe całych urządzeń, w tym danych i konfiguracji systemu



Cyberbezpieczny Samorząd

- Kopia zapasowa oparta na agencie tworzy kopie zapasowe i przywraca zmienione bloki znalezione między migawkami
- Korzystanie z funkcji śledzenia zmiany bloków Changed Block Tracking opartej na usłudze Microsoft VSS do tworzenia przyrostowych kopii zapasowych
- Zdarzenia tworzenia kopii zapasowych wyzwalane zdarzeniami obejmując blokadę ekranu urządzenia, wylogowanie użytkownika i uruchamianie urządzeń
- Okno kopii zapasowej umożliwiające dostosowywanie dozwolonego i niedozwolonego czasu tworzenia kopii zapasowej
- Obsługa wstawiania argumentów (adres IP serwera NAS, nazwa użytkownika, hasło i tworzenie ikony programu do backupu) do instalatora .msi w celu masowego wdrażania agenta oprogramowania do backupu

Serwer fizyczny (Windows)

Dane techniczne

- Obsługiwane platformy: Windows 11 (wszystkie wersje), Windows 10 (wszystkie wersje), Windows 8.1 (wszystkie wersje), Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 i Windows Server 2022
- Obsługa systemu plików NTFS
- Tryby tworzenia kopii zapasowych: Kopia zapasowa całego urządzenia, wolumenu systemowego i niestandardowego wolumenu
- Metody przywracania: Przywracanie całego urządzenia, przywracanie na poziomie plików/folderów, przywracanie na poziomie woluminów i natychmiastowe przywracanie do VMware vSphere, Microsoft Hyper-V
- Kopia zapasowa oparta na obrazie tworzy kopie zapasowe całych urządzeń, w tym danych i konfiguracji systemu
- Kopia zapasowa oparta na agencie tworzy kopie zapasowe zmienionych bloków znalezionych między migawkami
- Korzystanie z funkcji do śledzenia zmiany bloków Changed Block Tracking w oparciu o usługę Microsoft VSS w celu wykonywania przyrostowych kopii zapasowych
- Okno kopii zapasowej umożliwiające dostosowywanie dozwolonego i niedozwolonego czasu tworzenia kopii zapasowej
- Obsługa wstawiania argumentów (adres IP serwera NAS, nazwa użytkownika, hasło i tworzenie ikony programu do backupu) do instalatora .msi w celu masowego wdrażania agenta oprogramowania do backupu



Serwer fizyczny (Linux)

Dane techniczne

- Obsługuje wersje jądra pomiędzy 2.6 a 6.8
- Obsługiwane platformy: CentOS 7.8, 7.9, 8.1, 8.5; RHEL 8.1, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4; Fedora 38, 39, 40; Ubuntu 20.04, 22.04, 24.04; Debian 10, 11, 12
- Obsługiwane systemy plików: ext2, ext3, ext4, XFS
- Obsługiwane typy urządzeń: /dev/sdx, /dev/hdx, /dev/vdx, /dev/nvmex, /dev/mdx
- Tryby kopii zapasowej: Całe urządzenie, wolumen systemowy i dostosowana kopia zapasowa wolumenu
- Metody przywracania: Przywracanie całego urządzenia, przywracanie na poziomie plików/folderów, przywracanie oparte na wolumenie oraz natychmiastowe przywracanie do VMware vSphere, Microsoft Hyper-V
- Kopia zapasowa oparta na obrazach tworzy kopie całych urządzeń, w tym danych i konfiguracji systemu
- Kopia zapasowa oparta na agencie tworzy kopie zapasowe i przywraca zmienione bloki znalezione między migawkami
- Wykorzystuje śledzenie zmienionych bloków oparte na sterowniku migawki Linux do wykonywania kopii zapasowych przyrostowych
- Okno kopii zapasowej dla użytkowników do dostosowania dozwolonego i niedozwolonego czasu tworzenia kopii zapasowych

Serwer plików (SMB)

Dane techniczne

- Obsługiwany protokół SMB: SMB1, SMB2 i SMB3
- Tworzenie kopii zapasowych bez agentów
- Tryby tworzenia kopii zapasowych: Wiele wersji, kopia lustrzana i przyrostowe kopie zapasowe
- Metoda przywracania: Przywracanie na poziomie plików/folderów
- Obsługa tworzenia kopii zapasowych listy ACL systemu Windows
- Obsługa usługi Windows VSS w celu zapewnienia spójności danych kopii zapasowej
- Jednoczesne wykonywanie zadań kopii zapasowej

Serwer plików (rsync)





Cyberbezpieczny Samorząd

Dane techniczne

- Obsługa wersji rsync 3.0 lub nowszej
- Kopia zapasowa bez agentów
- Tryby kopii zapasowych: Wiele wersji, kopia lustrzana i przyrostowe kopie zapasowe
- Metoda przywracania: Przywracanie na poziomie pliku/folderu
- Obsługa tworzenia kopii zapasowej Linux POSIX ACL
- Obsługa trybu rsync module, trybu rsync shell przez SSH oraz trybu rsync module przez SSH
- Obsługa uwierzytelniania za pomocą hasła lub klucza SSH
- Obsługa transferu na poziomie bloku, szyfrowania i kontroli przepustowości
- Jednoczesne wykonywanie zadań tworzenia kopii zapasowych

Maszyna wirtualna

Dane techniczne

- Obsługiwane platformy VMware vSphere: VMware vSphere 5.0, 5.1, 5.5, 6.0, 6.5, 6.7 i 7.0 i 8.0
- Obsługiwane wersje VMware vSphere: VMware free ESXi, VMware vSphere Essentials, VMware vSphere Essentials Plus, VMware vSphere Standard, VMware vSphere Advanced, VMware vSphere Enterprise i VMware vSphere Enterprise Plus
- Obsługa wszystkich typów i wersji sprzętu wirtualnego VMware, w tym 62 TB VMDK
- Obsługa monitorów maszyny wirtualnej Microsoft Hyper-V: Hyper-V 2016, Hyper-V 2019 i Hyper-V 2022
- Obsługa oprogramowania Microsoft System Center Virtual Machine Manager (SCVMM): System Center Virtual Machine Manager 2016, System Center Virtual Machine Manager 2019
- Obsługa klastrów przełączania awaryjnego Microsoft Hyper-V: Hyper-V 2016, Hyper-V 2019 i Hyper-V 2022
- Obsługa maszyn wirtualnych Hyper-V generacji 1 i 2, w tym dysków VHDX o pojemności 64 TB i wersji sprzętu wirtualnego od 5.0 do 9.0
- W przypadku tworzenia kopii zapasowych Microsoft Hyper-V wymagany jest wolumen systemowy hosta z co najmniej 512 MB wolnego miejsca w celu zainstalowania narzędzia do przenoszenia danych



Cyberbezpieczny Samorząd

- Kopia zapasowa oparta na obrazie tworzy kopie zapasowe całych urządzeń, w tym konfiguracji danych i systemu
- Kopia zapasowa bez agentów
- Korzystanie z funkcji śledzenia zmienionych bloków VMware i funkcji Hyper-V Resilient Change Tracking do wykonywania przyrostowej kopii zapasowej
- Okno kopii zapasowej umożliwiające dostosowywanie dozwolonego i niedozwolonego czasu tworzenia kopii zapasowych
- Metody przywracania: Przywracanie całego urządzenia, przywracanie na poziomie plików/folderów i natychmiastowe przywracanie do VMware vSphere, Microsoft Hyper-V
- W przypadku przywracania na poziomie plików w systemie operacyjnym gościa obsługiwane systemy plików systemu Windows to NTFS i FAT32, a obsługiwane systemy plików systemu Linux to NTFS, FAT32, ext3, i ext4
- Obsługa tworzenia kopii zapasowych systemów operacyjnych i aplikacji obsługiwanych przez rozwiązania VMware vSphere i Microsoft Hyper-V

Portal przywracania

Funkcje

- Przywracanie pojedynczego pliku/folderu w celu zaoszczędzenia czasu przywracania
- Wyszukiwanie słów kluczowych użytkowników w celu łatwego znalezienia żądanych danych

Dane techniczne

- Przywracanie danych
 - Zbiornicze przywracanie pliku/folderu w tym samym katalogu
 - Przywracanie plików/folderów do nowych urządzeń (ten sam system operacyjny)
 - Możliwość przywracania danych kopii zapasowej fizycznych serwerów z systemem Windows/Linux, serwerów plików i maszyn wirtualnych należących do wersji kopii zapasowych zakończonych częściowym powodzeniem
 - Metadane pliku/folderu, które można przywracać, różnią się w zależności od przywracanych systemów:
 - Windows: Czas modyfikacji danych (mTime) i czas dostępu (aTime)



Cyberbezpieczny Samorząd

- Linux: Czas modyfikacji danych (mTime), czas dostępu (aTime), właściciel pliku i uprawnienia pliku (uprawnienia ACL)
- Virtual Machine: Czas modyfikacji danych (mTime), czas dostępu (aTime), czas utworzenia (cTime) i uprawnienia pliku (uprawnienia ACL), UID i GID
- Data download (Pobieranie danych)
 - Zbiorcze pobieranie pliku/folderu w tym samym katalogu
 - Plik/folder pobrany w pakiecie zostanie skompresowany do pojedynczego pliku
 - Możliwość pobierania danych kopii zapasowej fizycznych serwerów z systemem Windows/Linux, serwerów plików i maszyn wirtualnych należących do wersji kopii zapasowych zakończonych częściowym powodzeniem

Oprogramowanie agenta

Wymagane do zainstalowania na urządzeniu docelowym dla komputerów z systemem Windows, Mac i fizycznych serwerów z systemem Windows/Linux w celu wykonania kopii zapasowej i przywracania

- Wymagania systemowe
 - Windows
 - Obsługiwane platformy: Windows 11 (wszystkie edycje), Windows 10 Creators Update (wszystkie edycje), Windows 10 (wszystkie edycje), Windows 8.1 (wszystkie edycje), Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022
 - Obsługuje modele Windows z procesorami x86-64
 - Linux
 - Obsługiwane platformy: CentOS 7.8, 7.9, 8.1, 8.5; RHEL 6.10, 7.8, 7.9, 8.1, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4; Ubuntu 16.04, 18.04, 20.04, 22.04, 24.04; Fedora 38, 39, 40; Debian 10, 11, 12
 - Obsługuje modele Linux z procesorami x86-64
 - Wersja jądra musi być powyżej 2.6 i poniżej 6.8

Kreator nośników do odzyskiwania

Funkcje



Cyberbezpieczny Samorząd

- Umożliwia automatyczne tworzenie nośników do odzyskiwania systemu w celu przywracania woluminów/przywracania bare-metal dla komputerów z systemem Windows, komputerów Mac i serwerów fizycznych z systemem Windows/Linux

Dane techniczne

- Wymagania systemowe
 - Windows
 - Obsługiwane platformy: Windows 11 (wszystkie edycje), Windows 10 (wszystkie edycje), Windows Server 2022, Windows Server 2019, Windows Server 2016
 - Obsługuje modele Windows z procesorami x86-64
- Obsługiwane typy nośników: obrazy USB/ISO
- Wymagana jest co najmniej 2,5 GB pojemność wolumenu systemowego na pliki tymczasowe
- Wymagana jest co najmniej 1 GB pojemność dla napędu USB i wolumenu do przechowywania obrazów ISO

Kreator odzyskiwania

Umożliwia użytkownikom przywracanie danych z woluminów na komputerach z systemem Windows, komputerach Mac i fizycznych serwerach z systemem Windows/Linux dzięki nośnikom odzyskiwania tworzonym przez użytkowników

Usługa wdrożenia:

Usługa wdrożenia może zostać zrealizowana w siedzibie zamawiającego lub zdalnie, a w jej zakresie powinny zawierać się przynajmniej:

- Montaż, konfiguracja i podłączenie macierzy dyskowej NAS do sieci lokalnej LAN
- Instalacja i konfiguracja aplikacji serwera backupu na oferowanym urządzeniu
- Instalacja aplikacji klienta backupu na wybranych stacjach
- Omówienie i konfiguracja zadań backupu dla serwerów oraz najważniejszych stacji klienckich
- Instruktażowe szkolenie dla pracowników technicznych



Cyberbezpieczny Samorząd

Część nr 2: Oprogramowanie do zarządzania tożsamością i dostępem

Opis Przedmiotu Zamówienia – część numer 2

Zakup oprogramowania do zarządzania tożsamością i dostępem w Urzędzie Gminy Strawczyn

Mechanizm ma za zadanie poprawić znacznie poprawić bezpieczeństwo systemów poprzez zwiększenie kontroli nad dostępem, minimalizacją zagrożeń związanych z zarządzaniem hasłami i redukcję ryzyka ataków na konta użytkowników. Zapewnia centralne zarządzanie kontami użytkowników i dostępem do zasobów.

Dostępność i wydajność: Zapewnienie szybkiego i niezawodnego mechanizmu logowania, aby użytkownicy mogli rozpocząć pracę z systemem bez opóźnień i problemów technicznych.

Bezpieczne przechowywanie danych uwierzytelniających: Hasła i dane autoryzacyjne powinny być przechowywane w sposób bezpieczny z wykorzystaniem silnych algorytmów kryptograficznych, aby uniemożliwić odzyskanie oryginalnego hasła w przypadku naruszenia dostępu do systemu.

Odporność na ataki: Mechanizm logowania powinien ograniczać liczbę prób nieudanych logowań aby uniemożliwić lub utrudnić atakującemu próby odgadnięcia hasła metodą brute force (np. blokada po 3 nieudanych próbach na 5 minut).

Wymuszanie bezpieczeństwa: Mechanizm powinien umożliwić definiowanie własnej polityki bezpieczeństwa, tj. wymagania co do długości hasła, złożoności (np. wymóg zawierania wielkich liter, małych liter, cyfr i znaków specjalnych) oraz okresowej zmiany hasła.

Szyfrowanie danych: Wszystkie dane przesyłane w procesie logowania powinny być szyfrowane w celu ochrony przed przechwyceniem przez osoby trzecie.



Cyberbezpieczny Samorząd

Bezpieczne zarządzanie sesjami: Mechanizm powinien umożliwić ograniczenie czasu trwania sesji oraz usuwać ją całkowicie po wylogowaniu użytkownika.

Monitorowanie aktywności: Mechanizm powinien rejestrować i monitorować aktywność logowania, w tym udane i nieudane próby logowania, aby wykrywać potencjalne próby naruszenia bezpieczeństwa.

Współpraca: Mechanizm bezpiecznego logowania powinien mieć możliwość konfiguracji i uruchomienia z kontrolerem domeny na środowisku z systemem Windows Serwer (np. Windows Serwer 2022) oraz Linux (Debian ≥ 12). Stacja końcowa (kliencka) musi być wyposażona w system Windows wspierający integrację z domeną tj. Professional bądź Enterprise.

Zakres integracji z obecnym systemem dziedzicznym

W wyniku integracji mechanizmu bezpiecznego logowania z systemem dziedzicznym Respons autoryzacja użytkownika powinna nastąpić po uprzedniej skutecznej autoryzacji użytkownika na stacji roboczej, bez konieczności ponownego logowania bezpośrednio w systemie dziedzicznym.

Pojedyncze logowanie powinno wyeliminować konieczność posiadania wielu różnych kont przez użytkowników.

Integracja powinna być parametryzowana i opcjonalna.

Lista czynności dot. wdrożenia mechanizmu

Aktualizacja systemu dziedzicznego na potrzeby uruchomienia mechanizmu bezpiecznego logowania.

Wsparcie przy konfiguracji i mapowaniu użytkowników systemu dziedzicznego Respons z użytkownikami domeny.

Instruktaże oraz asystę stanowiskową dla administratora.

Świadczenie pomocy technicznej dotyczącej mechanizmu bezpiecznego logowania.

Świadczenie usług utrzymania i konserwacji dla dostarczonego mechanizmu.

Dostarczenie nowych wersji dokumentacji użytkownika wraz z nowymi wersjami systemu dziedzicznego i mechanizmu bezpiecznego logowania.

Okres gwarancji: 3 lata.