Załącznik nr 3 do SWZ

Szczegółowy opis przedmiotu zamówienia

1. Serwer (2 sztuki)

Lp.	Wymaganie
1.	Parametry fizyczne platformy
1.1	Obudowa serwerowa do montażu w szafie rack 19"
1.2	W zestawie szyny montażowe (rail kit) umożliwiające wysunięcie serwera w szafie bez jego demontażu
1.3	Zasilanie sieciowe 230V AC
1.4	Dwa redundantne zasilacze hot-swap o mocy min. 700 W każdy, klasy sprawności Platinum (94%) lub wyższej — wymiana podczas pracy serwera bez jego wyłączania; utrata jednego zasilacza nie powoduje przerwy w pracy serwera
2.	Procesor
2.1	Jeden procesor serwerowy w wykonaniu jednopodstawkowym (single-socket), min. 16 rdzeni fizycznych, min. 32 wątków logicznych; architektura 64-bitowa x86
2.2	Taktowanie bazowe min. 2,3 GHz
2.3	Cache LLC min. 16 MB
2.4	Obsługa instrukcji wirtualizacji sprzętowej (VT-x) oraz wirtualizacji We/Wy (VT-d)
3.	Pamięć operacyjna RAM
3.1	Pamięć zainstalowana: min. 64 GB DDR5 ECC
3.2	Taktowanie pamięci: min. 4400 MT/s
3.3	Konfiguracja modułów: 2× 32 GB— co najmniej 2 sloty wolne (platforma posiada co najmniej 4 sloty łącznie), umożliwiające rozbudowę bez wymiany istniejących modułów
3.4	Maksymalna obsługiwana pojemność RAM: min. 128 GB
3.5	Obsługa korekcji błędów ECC
4.	Podsystem dyskowy i RAID
4.1	Warstwa boot (system hypervisora): dwa dyski NVMe o pojemności min. 480 GB każdy, skonfigurowane w RAID 1
4.2	Warstwa danych produkcyjnych: cztery dyski SSD SAS 2,5" o pojemności min. 960 GB każdy, skonfigurowane w RAID 10 — minimalna pojemność netto 1,8 TB; przeznaczone dla maszyn wirtualnych, na bazy danych i systemy ERP
4.3	Warstwa danych pojemnościowych: dwa dyski HDD/SSD SAS 2,5" o pojemności min. 2,4 TB każdy, skonfigurowane w RAID 1 — minimalna pojemność netto 2,3 TB; przeznaczone dla archiwów, zasobów BIP i snapshotów maszyn wirtualnych
4.4	Wszystkie zatoki dyskowe w wykonaniu hot-swap — wymiana dysku podczas pracy serwera bez jego wyłączania; platforma musi obsługiwać min. 8 zatok 2,5" hot-plug w zatoce przedniej
4.5	Sprzętowy kontroler RAID obsługujący dyski SATA/SAS, z dedykowaną pamięcią podręczną (cache) min. 2 GB, z ochroną danych cache przez moduł bateryjny lub kondensatorowy (battery-backed / flash-backed write cache) — wymagany dla warstwy produkcyjnej RAID 10
4.6	Kontroler RAID obsługuje poziomy: RAID 0, 1, 5, 6, 10, 50, 60
5.	Interfejsy sieciowe
5.1	Min. dwa porty 1 GbE RJ45 wbudowane (LOM) — przeznaczone do sieci produkcyjnej i zarządzania; możliwość rozbudowy o kartę sieciową z portami 10 GbE SFP+ przez slot OCP lub PCIe lub rozwiązanie równoważne producenta.
5.2	Dedykowany port zarządzania zdalnego (BMC) RJ45 — fizycznie niezależny od portów produkcyjnych, dostępny w trybie out-of-band nawet przy wyłączonym systemie operacyjnym
6.	Zarządzanie zdalne
6.1	Wbudowany dedykowany kontroler zarządzania zdalnego klasy Enterprise (BMC) umożliwiający: zdalny dostęp KVM przez przeglądarkę internetową bez dodatkowego oprogramowania klienckiego, montowanie wirtualnych nośników (virtual media ISO/IMG), sterowanie zasilaniem i resetem, monitoring temperatury, napięć i prędkości wentylatorów w czasie rzeczywistym
6.2	Kontroler BMC musi posiadać własny dedykowany procesor, pamięć i kartę sieciową — niezależny od głównego procesora serwera; dostępny i w pełni funkcjonalny nawet przy awarii głównego systemu
6.3	Obsługa API RESTful zgodnego ze standardem DMTF Redfish — umożliwiającego automatyzację zarządzania i integrację z narzędziami klasy Infrastructure-as-Code (Ansible, Terraform lub równoważne)
6.4	Obsługa standardu IPMI 2.0 — zapewniającego kompatybilność z narzędziami monitoringu infrastruktury niezależnymi od producenta serwera

6.5	Obsługa SNMP v1–v3, SMTP (alerty e-mail), Syslog — do integracji z zewnętrznymi systemami monitoringu i SIEM
6.6	Port konsoli szeregowej (RS-232 lub USB) do lokalnego zarządzania awaryjnego
6.7	Możliwość zdalnej aktualizacji oprogramowania układowego (firmware) serwera i kontrolera BMC bez przerywania pracy serwera (gdzie technicznie możliwe)
7. Wirtualizacja i oprogramowanie	
7.1	Serwer (lub jego części) musi być oficjalnie wspierany przez producenta wybranego hypervisora lub figurować na liście kompatybilności producenta rozwiązania.
7.2	Obsługa sprzętowej wirtualizacji We/Wy (SR-IOV) dla kart sieciowych
7.3	Sprzętowy moduł TPM 2.0 wbudowany lub wymienny (musi być dostarczony) — wymagany dla bezpiecznego rozruchu hypervisora i szyfrowania woluminów maszyn wirtualnych
7.4	Obsługa Secure Boot oraz sprzętowej weryfikacji integralności firmware przy każdym uruchomieniu serwera
8. Parametry wydajnościowe	
8.1	Obsługa PCIe 4.0 lub nowszego — min. jeden slot PCIe x8 lub x16 full-height dostępny na rozbudowę
8.2	Obsługa min. 8 dysków 2,5" hot-plug w zatokach przednich oraz min. 2 dysków M.2/U.2/U.3 przeznaczonych na warstwę dysków boot
9. Bezpieczeństwo	
9.1	Sprzętowy moduł TPM 2.0 (wbudowany, lutowany lub w gnieździe dedykowanym)
9.2	Sprzętowa weryfikacja integralności firmware kontrolera BMC i BIOS/UEFI przy każdym uruchomieniu — uniemożliwiająca uruchomienie serwera ze zmodyfikowanym lub złośliwym firmware
10. Gwarancja i wsparcie	
10.1	Gwarancja producenta minimum 24 miesięcy w trybie On-Site Next Business Day (NBD) — naprawa lub wymiana wadliwego podzespołu u klienta następnego dnia roboczego od zgłoszenia
10.2	Serwis gwarancyjny realizowany na terenie Unii Europejskiej

2. Serwer NAS

Parametr	Opis
Obudowa	Rack
Procesor	Czterordzeniowy procesor o taktowaniu 2,2 GHz z obsługą AES-NI
Sprzętowy mechanizm szyfrowania	Tak (AES-NI)
Pamięć RAM	min. 4 GB pamięci ECC SODIMM z możliwością rozszerzenia do min. 32 GB
Możliwości rozbudowy	Sprzęt powinien być wyposażony w min. 8 kieszeni na dyski twarde typu hot-swap z możliwością rozszerzenia do 12 dysków łącznie przy użyciu dodatkowej jednostki rozszerzającej podłączanej do jednostki głównej za pomocą interfejsu przewidzianego przez producenta urządzenia (np. eSATA)
Porty zewnętrzne	Minimum: • 2 porty USB 3.1
Porty sieciowe	Minimum: • 2 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego) • karta sieciowa 10G zainstalowana w gnieździe rozszerzeń PCIe x8 lub wbudowana
Funkcja Wake on LAN/WAN	Tak
Gniazdo rozszerzeń PCIe 3.0	Min. 1x 4-liniowe gniazdo x8
Wentylator obudowy	Min. 2 wentylatory 80 mm x 80 mm
Obsługiwane protokoły sieciowe	Min. SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPS, FTP, SNMP, LDAP, CalDAV
Obsługiwane systemy plików	Min.: • Wewnętrzny: Btrfs lub ext4 lub równoważny system plików zapewniający obsługę migawek, sum kontrolnych oraz ochronę metadanych. Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT

Zarządzanie pamięcią masową	• Maksymalny rozmiar pojedynczego wolumenu: 108 TB • Minimalna liczba wewnętrznych wolumenów: 64 • Minimalna liczba obiektów iSCSI Target: 128 • Minimalna liczba jednostek iSCSI LUN: 256
	Obsługa klonowania/migawek jednostek iSCSI LUN
Dyski twarde	• 4 dyski HDD 7200 rpm, modele dedykowane dla NAS o wysokiej trwałości, min. 8 TB każdy • 2 dyski SSD, modele dedykowane dla NAS o wysokiej trwałości, min. 240 GB każdy
Obsługiwane typy macierzy RAID	Min. JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
Funkcja udostępniania plików	• Minimalna liczba kont użytkowników: 2 048 • Minimalna liczba grup użytkowników: 256 • Minimalna liczba folderów współdzielonych: 512 • Minimalna liczba jednoczesnych połączeń SMB/NFS/AFP/FTP: 1000
Uprawnienia	Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL)
Wirtualizacja	Obsługa VMware vSphere®, Microsoft Hyper-V®, Citrix®, OpenStack®
Usługa katalogowa	Łączy się z serwerami Windows® AD/LDAP, umożliwiając użytkownikom domeny logowanie za pośrednictwem protokołów SMB/NFS/AFP/FTP przy użyciu istniejących poświadczeń.
Bezpieczeństwo	Zapora, szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania)
Obsługiwane systemy klienckie	Windows®10 i nowsze, macOS® 10.12 i nowsze
Obsługiwane przeglądarki	Chrome®, Firefox®, Edge® i nowsze, Safari® 10 i nowsze, Safari (iOS 10 i nowsze), Chrome (Android™ 6.0 i nowsze) na tabletach
Oprogramowanie	• Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych, aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z repozytorium aplikacji producenta.
Konserwacja	Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwnych szyn rack
Zasilanie	Wymogiem jest dostarczenie sprzętu wyposażonego w nadmiarowy zasilacz
Gwarancja	• Minimum 2 lata gwarancji producenta na serwer NAS. • Minimum 2 lata gwarancji na zainstalowane dyski twarde. • Minimum 2 lata na dodatkowe akcesoria montażowe w postaci przesuwnych szyn rack • Serwis ma być świadczony w miejscu instalacji urządzeń (on-site). • Uszkodzone dyski pozostają własnością Zamawiającego.

3. UPS do serwera rack (1 sztuka)

Parametr	Opis
Typ urządzenia	Zasilacz awaryjny UPS, montaż rack 19", wysokość 2U, technologia line-interactive lub online VFI
Moc pozorna (VA)	Min. 3000 VA
Moc czynna (W)	Min. 2700 W (współczynnik mocy 0.9)
Topologia	Line-interactive z automatyczną regulacją napięcia (AVR) lub online VFI (double conversion)
Zakres napięcia wejściowego	160–294 V (regulowany do 150–280 V)
Zakres częstotliwości wejściowej	47–70 Hz (dla systemów 50 Hz), 56.5–70 Hz (dla 60 Hz), min. 40 Hz w trybie niskiej czułości
Złącze wejściowe	IEC C20, długość kabla min. 1.8 m

Napięcie wyjściowe	Nominalne 230 V (regulowane: 200/208/220/230/240 V), tolerancja +6%/-10%
Kształt napięcia wyjściowego	Czysta sinusoida
Gniazda wyjściowe	Min. 8 x IEC C13, 1 x IEC C19
Akumulatory	bezobsługowe, ołowiowo-kwasowe (VRLA), wymienialne przez użytkownika
Zarządzanie baterią	Zaawansowany system zarządzania baterią, ładowanie z kompensacją temperaturową, automatyczny test baterii, ochrona przed głębokim rozładowaniem, automatyczne rozpoznawanie modułów zewnętrznych
Możliwość rozbudowy baterii	Tak, obsługa zewnętrznych modułów bateryjnych
Czas podtrzymania	Zależny od obciążenia możliwość doboru konfiguracji zewnętrznych baterii (np. 5–15 min przy 100% obciążeniu)
Efektywność energetyczna	Dla urządzeń line-interactive: minimum 96% sprawności. Dla urządzeń online VFI: minimum 90% sprawności.
Porty komunikacyjne	USB (HID), złącze przekaźnikowe (dry contact), złącze do zdalnego włączania/wyłączania, slot rozszerzeń (z kartą sieciową w zestawie)
Zarządzanie i oprogramowanie	Wsparcie dla oprogramowania do zarządzania zasilaniem i zamykania systemów (np. równoważne do Eaton Intelligent Power Manager/Protector), SNMP, integracja z VMware, HyperV, Xen, Red Hat, Citrix
Zabezpieczenia	Ochrona przed przeciążeniem, zwarciem, przepięciem, przegrzaniem, ESD, przepięciami na linii danych
Chłodzenie i hałas	Wentylator z regulacją prędkości, poziom hałasu <40 dB (z odległości 1 m)
Warunki środowiskowe	Temperatura pracy: 0–40°C (zalecane max. 25°C dla baterii), wilgotność: minimum 20–80% (bez kondensacji), wysokość: do 1500 m n.p.m.
Wymiary	Max. 770 mm (głębokość) x 430 mm (szerokość) x 86 mm (wysokość 2U)
Waga	Max. 50 kg
Kolor i obudowa	Czarna/srebrna, metalowa obudowa rack 19"
Zawartość zestawu	UPS, karta sieciowa, kabel zasilający, zestaw montażowy rack, wsporniki do montażu wieżowego, kabel USB, przewody IEC, instrukcja szybkiego startu, instrukcje bezpieczeństwa
Certyfikaty i zgodność	CE, LVD (Low Voltage Directive), EMC (Electromagnetic Compatibility), RoHS, REACH, IEC/EN 62040-1/2/3 oraz inne równoważne certyfikaty wymagane do legalnego wprowadzenia urządzenia do obrotu na terenie Unii Europejskiej.
Gwarancja i wsparcie techniczne	Min. 2 lata gwarancji na elektronikę, min. 2 lata na baterie, z możliwością rozszerzenia do 5 lat. Wsparcie techniczne producenta lub autoryzowanego partnera, dostęp do aktualizacji firmware, dokumentacji, portalu wsparcia. Serwis w trybie NBD (Next Business Day). W przypadku awarii baterii lub komponentów możliwość zatrzymania wadliwego nośnika (np. baterii) przez klienta bez konieczności zwrotu.
Dokumentacja	Wymagane jest dostarczenie pełnej dokumentacji technicznej w języku polskim, obejmującej: instrukcję instalacji i konfiguracji, opis funkcji i interfejsów, procedury bezpieczeństwa, instrukcje aktualizacji firmware i obsługi oprogramowania zarządzającego.
Dodatkowe wymagania	Możliwość integracji z systemami monitoringu infrastruktury IT, obsługa automatycznego zamykania systemów operacyjnych, możliwość pracy w konfiguracji redundantnej (np. z bypassem), możliwość montażu w szafach o głębokości min. 800 mm.

4. Narzędzia do wirtualizacji

Lp.	Wymaganie
1.	Typ i architektura platformy wirtualizacji
1.1	Platforma wirtualizacji klasy Type 1, działająca bezpośrednio na sprzęcie fizycznym, dostarczona jako funkcja serwerowego systemu operacyjnego lub jako rozwiązanie równoważne funkcjonalnie. Platforma musi umożliwiać uruchamianie i zarządzanie maszynami wirtualnymi w środowisku zgodnym z wymaganiami Zamawiającego, w szczególności z obsługą systemów Windows Server, usług katalogowych, usług pulpitu zdalnego, mechanizmów bezpiecznego rozruchu, wirtualnego TPM, kopii migawkowych, migracji oraz replikacji maszyn wirtualnych.
1.2	Obsługa maszyn wirtualnych opartych na firmware UEFI, z obsługą Secure Boot oraz wirtualnego modułu TPM 2.0 lub mechanizmów równoważnych dla każdej VM.
1.3	Zarządzanie maszynami wirtualnymi możliwe z poziomu graficznego interfejsu zarządczego (GUI) dostępnego lokalnie lub zdalnie, a także z poziomu wiersza poleceń (CLI/PowerShell)
1.4	Zarządzanie zdalne przez dedykowane narzędzia administracji serwerami dostępne na stacjach roboczych administratora (RSAT lub równoważne) — bez konieczności logowania się bezpośrednio na serwer

2. Wymagania sprzętowe hosta

2.1 Procesor 64-bitowy z obsługą sprzętowej wirtualizacji (Intel VT-x lub AMD-V) oraz translacji adresów drugiego poziomu (SLAT: Intel EPT lub AMD RVI/NPT)

2.2 Obsługa sprzętowego wymuszania zasady DEP (Data Execution Prevention) — Intel XD bit lub AMD NX bit

2.3 Minimalna ilość pamięci RAM hosta: 8 GB (zalecane min. 128 GB dla środowiska produkcyjnego z wieloma VM)

2.4 Minimum 64 GB wolnej przestrzeni dyskowej na partycji systemowej hosta (zalecane oddzielne wolumeny na system hosta i pliki VM)

3. Parametry skalowalności maszyn wirtualnych

3.1 Obsługa pamięci dynamicznej (Dynamic Memory) — automatyczne dostosowywanie przydziału RAM do VM w zależności od bieżącego obciążenia

3.2 Maksymalna pojemność pojedynczego wirtualnego dysku twardego lub równoważnego pliku/obiektu dyskowego VM: min. 64 TB.

3.3 Obsługa do 256 dysków SCSI i 4 kontrolerów SCSI na maszynę wirtualną

3.4 Obsługa do 68 wirtualnych kart sieciowych na maszynę wirtualną

4. Sieć wirtualna i przełączniki

4.1 Wbudowany przełącznik wirtualny (Virtual Switch) obsługujący tryby: zewnętrzny, wewnętrzny i prywatny — umożliwiający izolację ruchu sieciowego VM

4.2 Obsługa akceleracji sieciowej SR-IOV (Single Root I/O Virtualization) — bezpośredni dostęp VM do fizycznej karty sieciowej z pominięciem warstwy hypervisora, minimalizacja opóźnień sieciowych

4.3 Obsługa wirtualizacji sieciowej (NVGRE, VXLAN) do tworzenia izolowanych sieci wirtualnych między VM niezależnie od fizycznej topologii sieci

4.4 Obsługa Quality of Service (QoS) dla ruchu sieciowego VM — możliwość ograniczenia i gwarantowania przepustowości per VM lub per wirtualna karta sieciowa

5. Bezpieczeństwo maszyn wirtualnych

5.1 Obsługa wirtualnego modułu TPM 2.0 (vTPM) dla każdej VM — umożliwia szyfrowanie dysku VM algorytmem BitLocker lub równoważnym bez dostępu do fizycznego TPM hosta

5.2 Obsługa Secure Boot dla maszyn wirtualnych opartych o firmware UEFI.

5.3 Obsługa chronionych maszyn wirtualnych — szyfrowanie stanu i konfiguracji VM uniemożliwiające odczyt danych przez administratora hosta

5.4 Izolacja środowisk maszyn wirtualnych — brak możliwości dostępu jednej VM do zasobów pamięci lub dysku innej VM bez jawnej zgody administratora

6. Wysoka dostępność i ciągłość działania

6.1 Obsługa migracji na żywo (Live Migration) — przenoszenie działającej VM między hostami bez przerwy w pracy i bez utraty połączeń sieciowych

6.2 Obsługa Quick Migration — szybka migracja VM przy minimalnym czasie przestoju (alternatywa dla Live Migration w środowiskach bez współdzielonego storage)

6.3 Obsługa punktów kontrolnych (Checkpoints / Snapshots) — możliwość przywrócenia VM do dowolnego wcześniejszego stanu; obsługa zarówno standardowych, jak i punktów kontrolnych zgodnych z produkcją (Production Checkpoints, VSS-based)

6.4 Obsługa migracji danych maszyn wirtualnych pomiędzy lokalizacjami pamięci masowej bez konieczności zatrzymywania VM.

6.5 Obsługa replikacji maszyn wirtualnych do zapasowego hosta lub równoważnego mechanizmu replikacji/asynchronicznego odtwarzania VM w lokalizacji zapasowej.

7. Obsługiwane systemy operacyjne gości (VM)

7.1 Wsparcie dla gościnnych systemów operacyjnych: Windows Server 2016/2019/2022/2025, Windows 10/11, Linux (Ubuntu, Red Hat Enterprise Linux, Debian, SUSE, CentOS i inne dystrybucje) — z pełnymi usługami integracji (Integration Services)

7.2 Obsługa usług integracyjnych lub mechanizmów równoważnych zapewniających synchronizację czasu, spójny backup i zarządzanie VM.

8. Licencjonowanie platformy wirtualizacji i systemów gościnnych

8.1 Platforma wirtualizacji musi być dostarczona i licencjonowana w sposób umożliwiający legalne uruchamianie maszyn wirtualnych przewidzianych w niniejszym zamówieniu.

8.2 Dostarczone licencje muszą obejmować prawo do uruchomienia serwerowego systemu operacyjnego na każdym z dwóch dostarczanych serwerów fizycznych oraz prawo do uruchamiania co najmniej dwóch wirtualnych instancji serwerowego systemu operacyjnego na każdym w pełni zlicencjonowanym hoście.

8.3 Licencjonowanie musi być zgodne z aktualnymi zasadami producenta oferowanego systemu operacyjnego i platformy wirtualizacji, w szczególności z modelem licencjonowania rdzeni fizycznych, jeżeli taki model jest wymagany przez producenta.

8.4 Zamawiający planuje uruchomienie łącznie 4 maszyn wirtualnych z serwerowym systemem operacyjnym na dwóch hostach objętych zamówieniem. Wykonawca musi dostarczyć licencje w zakresie umożliwiającym legalne uruchomienie takiego środowiska.

9. Zarządzanie i monitorowanie

9.1	Centralne zarządzanie wieloma hostami wirtualizacji możliwe z poziomu dedykowanej konsoli zarządczej (Windows Admin Center lub równoważnej) dostępnej przez przeglądarkę — bez konieczności instalowania klienta na stacjach administratorów
9.2	Obsługa automatyzacji i skryptowania przez wbudowany interfejs wiersza poleceń, w szczególności PowerShell lub równoważny mechanizm automatyzacji, umożliwiający zarządzanie VM, przełącznikami wirtualnymi, dyskami i migracją.
9.3	Obsługa protokołu WMI/CIM do integracji z zewnętrznymi systemami monitoringu i zarządzania (SCCM, SCOM lub równoważne)
9.4	Wbudowane narzędzia do monitorowania wydajności VM i hosta: Menedżer zasobów, liczniki wydajności dostępne przez narzędzia monitoringu systemu operacyjnego

5. System Operacyjny Serwera (2 sztuki)

Lp.	Wymaganie
1.	Wersja i cykl życia
1.1	Serwerowy system operacyjny w najnowszej dostępnej, długoterminowo wspieranej wersji producenta, dostarczony wraz z serwerem, zapewniający możliwość budowy środowiska domenowego zgodnego funkcjonalnie z Microsoft Active Directory, Group Policy, usługi pulpitu zdalnego RDS, mechanizmami uwierzytelniania Kerberos/NTLM, SMB oraz licencjami dostępowe CAL/RDS CAL. Zamawiający posiada środowisko stacji roboczych Microsoft Windows oraz planuje wykorzystanie usług katalogowych, zasad grupowych, zdalnego dostępu RDS i integracji z systemami bezpieczeństwa objętymi niniejszym zamówieniem. Zamawiający dopuszcza rozwiązanie równoważne wyłącznie pod warunkiem zapewnienia pełnej zgodności funkcjonalnej, administracyjnej, integracyjnej i licencyjnej z wymaganiami określonymi w niniejszej specyfikacji, bez konieczności wymiany istniejących stacji roboczych, mechanizmów logowania użytkowników ani modelu licencjonowania dostępu użytkowników.
1.2	System musi zapewniać wsparcie producenta przez okres nie krótszy niż 10 lat od daty premiery.
1.3	Wymagane jest dostarczenie licencji serwerowego systemu operacyjnego obejmującej prawa do uruchomienia co najmniej 2 wirtualnych instancji serwerowego systemu operacyjnego na każdym w pełni zlicencjonowanym hoście fizycznym oraz spełniającej wymagania platformy wirtualizacji określone w pkt 4.
1.4	Dwa warianty instalacji do wyboru: instalacja z graficznym interfejsem użytkownika (Desktop Experience) oraz instalacja minimalna bez lokalnego GUI (Server Core) — zarządzana zdalnie przez przeglądarkę lub wiersz poleceń
2.	Wymagania sprzętowe
2.1	Procesor 64-bitowy (x64), min. 1,4 GHz, z obsługą zestawu instrukcji: NX/DEP, CMPXCHG16b, LAHF/SAHF, PrefetchW, SSE4.2 z instrukcją POPCNT oraz translacji adresów drugiego poziomu (SLAT: Intel EPT lub AMD NPT/RVI)
2.2	Minimalna ilość pamięci RAM: 512 MB (instalacja Server Core) / 2 GB (instalacja z GUI); zalecane min. 8 GB dla środowisk produkcyjnych; pamięć ECC zalecana dla fizycznych hostów
2.3	Minimalna przestrzeń dyskowa dla partycji systemowej: 32 GB; zalecane min. 64 GB, szczególnie przy ilości RAM powyżej 16 GB (pliki stronicowania, hibernacja, zrzuty pamięci)
2.4	Karta sieciowa zgodna ze standardem PCI Express, min. 1 Gbps przepustowości
2.5	Kontroler pamięci masowej zgodny ze standardem PCI Express; napędy typu HDD nie mogą korzystać z interfejsu PATA/IDE
2.6	Firmware UEFI w wersji min. 2.3.1c z obsługą Secure Boot
2.7	Fizyczny moduł TPM 2.0 (Trusted Platform Module) — wymagany dla funkcji szyfrowania dysków, ochrony poświadczeń użytkowników oraz mechanizmów zabezpieczeń opartych o sprzętowe źródło zaufania.
2.8	Urządzenie graficzne i monitor obsługujące rozdzielczość min. 1024×768 px (dotyczy wariantu z GUI)
3.	Usługi katalogowe i zarządzanie tożsamością
3.1	Wbudowana usługa katalogowa zapewniająca centralne zarządzanie użytkownikami, komputerami, grupami i politykami bezpieczeństwa, umożliwiająca budowę środowiska Microsoft Active Directory zgodnego z wymaganiami Zamawiającego.
3.2	Obsługa aktualnych poziomów funkcjonalności domeny i lasu dostępnych dla oferowanej wersji systemu operacyjnego.
3.3	Obsługa zarządzanych kont usługowych lub równoważnego mechanizmu automatycznego zarządzania poświadczeniami kont usługowych.
3.4	Wbudowane rozwiązanie do zarządzania hasłami lokalnych administratorów (LAPS) — automatyczne generowanie i rotacja unikalnych haseł lokalnych kont administracyjnych z przechowywaniem w usłudze katalogowej
3.5	Obsługa protokołu Kerberos w rozszerzonym zakresie scenariuszy uwierzytelniania; obsługa szyfrowania AES dla operacji zmiany haseł; blokada starszych algorytmów szyfrowania (DES, RC4) tam, gdzie jest to możliwe
4.	Usługi sieciowe i dostęp do zasobów
4.1	Wbudowana usługa DNS (Domain Name System) umożliwiająca rozwiązywanie nazw w środowisku lokalnym i integrację z usługą katalogową (Dynamic DNS, strefy zintegrowane z AD)
4.2	Wbudowana usługa DHCP (Dynamic Host Configuration Protocol) do automatycznego przydzielania adresów IP stacjom roboczym i urządzeniom sieciowym

4.3	Wbudowana usługa plików i udostępniania zasobów (File and Storage Services) z obsługą protokołu SMB 3.x; obsługa szyfrowania SMB wymaganego domyślnie dla wszystkich połączeń wychodzących
4.4	Obsługa bezpiecznego dostępu do zasobów plikowych przez sieci niezaufane z wykorzystaniem szyfrowania transmisji, np. SMB over QUIC lub rozwiązania równoważnego.
4.5	Wzmocnione domyślne reguły zapory sieciowej dla SMB — eliminacja portów NetBIOS (137–139) z domyślnych reguł udostępniania plików; ochrona przed atakami brute-force na uwierzytelnianie SMB (SMB authentication rate limiter)
4.6	Wbudowany serwer i klient OpenSSH — dostępny domyślnie, bez konieczności ręcznej instalacji; umożliwia bezpieczne zdalne zarządzanie serwerem przez SSH
4.7	Obsługa usług pulpitu zdalnego (Remote Desktop Services — RDS) umożliwiających zdalny dostęp użytkowników do aplikacji i pulpitów; wymaga dodatkowych licencji dostępu RDS CAL
4.8	Obsługa serwera zasad sieciowych (NPS — Network Policy Server) do uwierzytelniania sieciowego z protokołem RADIUS — integracja z kontrolą dostępu do sieci (NAC)
5.	Bezpieczeństwo systemu operacyjnego
5.1	Obsługa mechanizmów zabezpieczenia uruchamiania i integralności systemu obejmujących co najmniej Secure Boot, TPM 2.0 oraz izolację opartą o wirtualizację lub mechanizmy równoważne.
5.2	Obsługa izolacji danych uwierzytelniających w celu ochrony przed kradzieżą poświadczeń, np. Credential Guard lub mechanizm równoważny.
5.3	Obsługa szyfrowania dysków systemowych i danych z wykorzystaniem TPM 2.0, np. BitLocker lub mechanizm równoważny.
5.4	Obsługa szyfrowania połączeń LDAP z wykorzystaniem TLS oraz możliwość wymuszania szyfrowanej komunikacji z usługą katalogową.
5.5	Wbudowany mechanizm zarządzania politykami bezpieczeństwa — centralnie dystrybuowane i wymuszane ustawienia bezpieczeństwa dla wszystkich stacji roboczych i serwerów w domenie
5.6	Dostępność rekomendowanych profili lub bazowych konfiguracji bezpieczeństwa producenta systemu, możliwych do zastosowania po instalacji systemu.
6.	Zarządzanie i automatyzacja
6.1	Graficzna konsola zarządzania serwerem do lokalnego i zdalnego zarządzania rolami, funkcjami i konfiguracją serwera
6.2	Przeglądarkowa konsola zarządzania (Windows Admin Center lub równoważna) umożliwiająca zdalne zarządzanie serwerem, maszynami wirtualnymi i klastrem bez instalowania oprogramowania klienckiego na stacjach administratorów
6.3	Wbudowany interfejs wiersza poleceń (np. PowerShell, bash) z pełnym zestawem poleceń cmdlet do automatyzacji zadań administracyjnych, zarządzania rolami, politykami i infrastrukturą wirtualizacji
6.4	Obsługa protokołu SNMP (v1–v3) oraz WMI/CIM do integracji z zewnętrznymi systemami monitoringu i zarządzania infrastrukturą
7.	Aktualizacje i patching
7.1	Obsługa uaktualnień in-place (upgrade) z poprzednich wersji serwerowego systemu operacyjnego (co najmniej z wersji 2012 R2 i późniejszych) bez konieczności czystej instalacji i migracji ról
8.	Wydajność i pamięć masowa
8.1	Obsługa systemu plików zoptymalizowanego pod kątem dużych plików i środowisk wirtualizacyjnych, z mechanizmem szybkiego klonowania bloków lub równoważnym.
8.2	Obsługa replikacji danych między serwerami lub klastrami z możliwością ograniczenia wykorzystania pasma, np. przez kompresję transmisji lub mechanizm równoważny.
8.3	Obsługa akceleracji sieciowej SR-IOV dla maszyn wirtualnych w środowisku wirtualizacji — redukcja opóźnień sieciowych i obciążenia CPU hosta przez bezpośredni dostęp VM do fizycznej karty sieciowej
9.	Licencjonowanie
9.1	Dostarczone licencje muszą obejmować wszystkie rdzenie fizyczne każdego oferowanego serwera zgodnie z zasadami licencjonowania producenta oferowanego systemu operacyjnego.
9.2	Dostarczony zakres licencji musi umożliwiać legalne uruchomienie serwerowego systemu operacyjnego na dwóch hostach fizycznych oraz łącznie co najmniej czterech maszyn wirtualnych z serwerowym systemem operacyjnym.
9.3	Wymagane licencje dostępu klienta (CAL) dla każdego użytkownika lub urządzenia uzyskującego dostęp do usług serwerowego systemu operacyjnego; oddzielne licencje CAL wymagane dla usług pulpitu zdalnego (RDS CAL)
9.4	Licencja obejmuje prawo do downgrade — możliwość uruchomienia wcześniejszej wersji serwerowego systemu operacyjnego na podstawie licencji na wersję aktualną

6. Licencje dostępowe do serwera (30 sztuk; CAL i RDS CAL)

Lp.	Wymaganie
1.	Definicja i obowiązek posiadania licencji dostępu

1.1	Licencja dostępu klienta (CAL — Client Access License) jest wymagana dla każdego użytkownika lub urządzenia uzyskującego dostęp do usług serwerowego systemu operacyjnego, niezależnie od sposobu dostępu (bezpośredni, zdalny, przez aplikację pośredniczącą) i liczby serwerów w środowisku
1.2	Licencje CAL mają charakter sieciowy (per-środowisko), nie per-serwer — jeżeli użytkownik uzyskuje dostęp do wielu serwerów w tej samej domenie, wystarczy jedna licencja CAL dla tego użytkownika (nie mnoży się liczby CAL przez liczbę serwerów)
2.	Wersja licencji CAL
2.1	Licencje CAL muszą odpowiadać wersji serwerowego systemu operacyjnego lub być od niej nowsze — licencje CAL dla wcześniejszych wersji systemu operacyjnego nie uprawniają do dostępu do nowszych wersji serwera
2.2	Licencje CAL w najnowszej wersji muszą umożliwiać korzystanie również ze wspieranych wcześniejszych wersji serwerowego systemu operacyjnego zgodnie z zasadami licencjonowania producenta.
2.3	Licencje CAL są wieczyste (perpetual) — nie wymagają corocznego odnawiania dla danej wersji systemu operacyjnego; obowiązek zakupu nowych CAL pojawia się wyłącznie przy przejściu na nowszą wersję systemu operacyjnego serwera
3.	Typy licencji CAL — podstawowy dostęp do serwera
3.1	Licencja CAL per użytkownik (User CAL) — przypisywana do konkretnej osoby; uprawnia tę osobę do dostępu do usług serwera z dowolnej liczby urządzeń (komputer stacjonarny, laptop, tablet, smartfon); zalecana gdy liczba urządzeń przewyższa liczbę użytkowników lub gdy użytkownicy pracują zdalnie z wielu lokalizacji
3.2	Licencja CAL per urządzenie (Device CAL) — przypisywana do konkretnego urządzenia; uprawnia dowolną liczbę użytkowników do dostępu do usług serwera z tego urządzenia; zalecana gdy jedno urządzenie jest współdzielone przez wielu pracowników (np. stanowiska zmianowe, terminale, kioski); implementacja wymaga środowiska domenowego (Active Directory)
4.	Dodatkowe licencje CAL — usługi pulpitu zdalnego (RDS CAL)
4.1	Dostęp do usług pulpitu zdalnego (Remote Desktop Services — RDS) umożliwiających zdalną pracę użytkowników na graficznym pulpicie lub zdalnych aplikacjach serwera wymaga dodatkowej licencji RDS CAL — ponad standardowy CAL dostępu do serwera
4.2	RDS CAL dostępna w dwóch wariantach: per użytkownik (RDS User CAL) i per urządzenie (RDS Device CAL) — analogicznie do standardowych CAL; wybór wariantu zależny od modelu pracy użytkowników
4.3	RDS CAL musi odpowiadać wersji serwera pełniącego rolę hosta sesji pulpitu zdalnego. Dostępne jest prawo do downgrade (nowsza RDS CAL → starszy RD Session Host)
4.4	Standardowy CAL dostępu do serwera (pkt 3.1 i 3.2) nie zastępuje RDS CAL — oba rodzaje licencji są wymagane łącznie przy korzystaniu z usług pulpitu zdalnego
5.	Ilość licencji wymaganych w zamówieniu
5.1	**Wymagane jest 30 licencji CAL w trybie per użytkownik**
5.2	**Wymagane jest 30 licencji RDS CAL w trybie per użytkownik**
5.3	**Licencje muszą odpowiadać wersji dostarczonego serwerowego systemu operacyjnego albo być od niej nowsze, zgodnie z zasadami licencjonowania producenta.**
6.	Wyłączenia z obowiązku posiadania licencji CAL
6.1	Dostęp anonimowy do publicznych usług webowych (strony internetowe bez logowania) — CAL nie jest wymagany
6.2	Korzystanie z usług rozwiązywania nazw (DNS) i automatycznego przydzielania adresów IP (DHCP) przez urządzenia sieciowe — CAL nie jest wymagany
6.3	Urządzenia drukujące przez kolejkę wydruku zarządzaną przez serwer nie wymagają CAL wyłącznie za tę czynność — jednak użytkownik korzystający z innych usług serwera nadal wymaga CAL

7. Oprogramowanie do backupu (licencja wieczysta)

Lp.	Wymaganie
1.	Model licencjonowania i dostawa
1.1	Oprogramowanie dostarczane w modelu licencji wieczystej (perpetual) — jednorazowa opłata licencyjna bez obowiązkowych opłat subskrypcyjnych; oprogramowanie pozostaje w użytkowaniu bezterminowo po zakończeniu okresu wsparcia
1.2	Licencja obejmuje prawo do użytkowania oprogramowania przez czas nieokreślony; aktualizacje i wsparcie techniczne dostępne opcjonalnie jako odrębna usługa odnawiana niezależnie od licencji
1.3	Możliwość rozszerzenia licencji (upgrade edycji lub dodanie licencjonowanych jednostek) bez konieczności ponownej instalacji lub migracji konfiguracji i zadań backupowych
1.4	Oprogramowanie wdrażane wyłącznie on-premise na infrastrukturze zamawiającego — bez przymusu korzystania z infrastruktury chmurowej producenta
1.5	W ramach zamówienia dostarczane: licencja na serwer backup (2 hosty) oraz licencja na backup stacji roboczych (30 stacji roboczych Windows/Linux)
2.	Licencja — serwer backup maszyn wirtualnych

2.1 Licencja musi umożliwiać ochronę wszystkich maszyn wirtualnych uruchomionych na dwóch hostach objętych zamówieniem w cz. I.

2.2 Licencja przenaszalna — możliwość przypisania do innego hosta wirtualizacji bez dodatkowych opłat

2.3 Obsługiwane platformy wirtualizacji: co najmniej Microsoft Hyper-V, VMware vSphere i Proxmox VE

3. Licencja — backup stacji roboczych

3.1 Licencja wieczysta na backup fizycznych stacji roboczych — wymagana liczba: 30 stacji roboczych

3.2 Obsługiwane systemy operacyjne stacji roboczych: Windows 10/11 oraz dystrybucje Linux (Debian, Ubuntu, CentOS/RHEL lub równoważne)

3.3 Agent backupu stacji roboczych zarządzany z tej samej konsoli administracyjnej co backup maszyn wirtualnych — jeden interfejs dla całego środowiska

4. Funkcje backupu maszyn wirtualnych

4.1 Backup obrazowy maszyn wirtualnych (image-based, agentless) z wykorzystaniem mechanizmów snapshotów hypervisora — bez konieczności instalowania agenta wewnątrz VM

4.2 Backup inkrementalny oparty na śledzeniu zmienionych bloków (CBT — Changed Block Tracking) — minimalizacja okna backupowego i zużycia pasma

4.3 Granularne odzyskiwanie danych: możliwość przywrócenia pojedynczych plików lub folderów z backupu VM bez konieczności przywracania całej maszyny wirtualnej

4.4 Natychmiastowe uruchomienie VM (Instant VM Recovery) bezpośrednio z repozytorium backupu — minimalizacja czasu przestoju

4.5 Obsługa aplikacji świadomych VSS (Microsoft SQL Server, Active Directory, Exchange) — spójny backup na poziomie aplikacji

4.6 Replikacja maszyn wirtualnych do lokalizacji zapasowej (opcjonalnie) jako element strategii disaster recovery

5. Funkcje backupu stacji roboczych

5.1 Backup całego systemu stacji roboczej (bare metal / image-based) umożliwiający odtworzenie pełnego środowiska pracy użytkownika

5.2 Backup wybranych plików i folderów z możliwością definiowania harmonogramów i polityk retencji osobno dla każdej stacji lub grupy stacji

5.3 Granularne odzyskiwanie pojedynczych plików i folderów ze stacji roboczej bez konieczności przywracania całego obrazu systemu

5.4 Centralny monitoring statusu zadań backupu wszystkich stacji roboczych z poziomu konsoli administracyjnej

6. Bezpieczeństwo i ochrona danych

6.1 Szyfrowanie backupów algorytmem AES-256 — zarówno danych w repozytorium (at-rest), jak i podczas transmisji do repozytorium (in-transit); funkcja dostępna w ramach licencji bez dodatkowych opłat

6.2 Obsługa repozytoriów backupu z niezmiennością danych (immutability) — zabezpieczenie kopii zapasowych przed modyfikacją lub usunięciem przez ransomware lub nieautoryzowanego użytkownika

6.3 Obsługa rotacji nośników wymiennych (rotated drives) jako repozytorium backupu — umożliwiająca realizację strategii backup 3-2-1 z kasetami RDX lub podobnymi nośnikami wymiennymi

6.4 Kontrola dostępu oparta na rolach (RBAC) — możliwość zdefiniowania różnych poziomów uprawnień dla administratorów i operatorów backupu (minimum predefiniowane role Administrator i Obserwator)

6.5 Uwierzytelnianie dwuskładnikowe (2FA) dla dostępu do konsoli administracyjnej

7. Wdrożenie i zarządzanie

7.1 Instalacja i zarządzanie wyłącznie on-premise — na serwerze zamawiającego z systemem Windows Server lub Linux; możliwość wdrożenia jako wirtualny appliance (OVF/OVA) na hoście wirtualizacji

7.2 Interfejs zarządzania dostępny przez przeglądarkę internetową (HTTPS) bez konieczności instalowania dedykowanego klienta na stacjach administratora

7.3 Automatyczne harmonogramowanie zadań backupu z możliwością definiowania okien backupowych, polityk retencji i reguł powiadamiania

7.4 Powiadomienia e-mail o statusie zadań backupu (sukces, ostrzeżenie, błąd) z możliwością integracji z serwerem SMTP zamawiającego

7.5 Obsługa deduplikacji i kompresji danych w repozytorium — redukcja zajętości przestrzeni dyskowej przez kopie zapasowe

7.6 Możliwość weryfikacji integralności kopii zapasowych (backup verification) — automatyczne testowanie możliwości odtworzenia danych bez ingerencji administratora

8. Wsparcie techniczne i aktualizacje

8.1 W ramach zamówienia: minimum 12 miesięcy wsparcia technicznego producenta w dni robocze (Standard Support) — od daty dostarczenia licencji

8.2 W okresie aktywnego wsparcia: dostęp do aktualizacji oprogramowania (poprawki bezpieczeństwa i nowe wersje) bez dodatkowych opłat

8.3 Po wygaśnięciu wsparcia: możliwość dalszego użytkowania oprogramowania w posiadanej wersji bez żadnych dodatkowych opłat; odnowienie wsparcia opcjonalne i niezależne

8. Organizacja realizacji zamówienia

a) Komunikacja w ramach niniejszego zamówienia oraz podczas jego realizacji może odbywać się telefonicznie, poprzez komunikatory, ale wszelkie uzgodnienia w zakresie realizacji przedmiotu muszą być uzgadniane pomiędzy stronami pisemnie, w tym elektronicznie, poprzez wymianę informacji pocztą elektroniczną na wskazane adresy email.
b) Wykonawca ma obowiązek ścisłej współpracy z Zamawiającym na każdym etapie realizacji zamówienia.
c) Wykonawca winien uwzględniać wszelkie uwagi Zamawiającego, które doprecyzowują lub uzupełniają zapisy w SWZ i nie są z nimi sprzeczne.
d) W niniejszym dokumencie opisano wymagania minimalne.
e) W przypadku oferowania oprogramowania open source, jest to dopuszczalne pod warunkiem spełnienia warunku zapewnienia min. rocznego płatnego okresu wsparcia
f) Wszelkie nazwy własne technologii, standardów, producentów lub produktów użyte w dokumentacji należy interpretować jako przykładowe, o ile nie wynikają z wymagań kompatybilności z istniejącą infrastrukturą Zamawiającego. Zamawiający dopuszcza rozwiązania równoważne spełniające wymagania funkcjonalne, techniczne, administracyjne, integracyjne i licencyjne określone w niniejszym dokumencie.
g) Za rozwiązanie równoważne uznaje się rozwiązanie realizujące wymagane funkcjonalności, bezpieczeństwo, integrację i sposób eksploatacji określone w niniejszym dokumencie, niezależnie od zastosowanej architektury technicznej, nazewnictwa funkcji lub podziału funkcjonalności pomiędzy moduły i komponenty.
h) W przypadku rozwiązań równoważnych obowiązek wykazania równoważności spoczywa na Wykonawcy.