

Załącznik nr 3a do SWZ

Szczegółowy opis przedmiotu zamówienia – część I Sprzęt serwerowy

1. Serwer – zakup i wdrożenie (2 sztuki)

Lp.	Wymaganie
1.	Parametry fizyczne platformy
1.1	Obudowa serwerowa do montażu w szafie rack 19", wysokość maksymalnie 1U
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
1.5	MTBF powyżej 10 lat
2.	Procesor
2.1	Jeden procesor serwerowy klasy entry Xeon (lub równoważny) w wykonaniu jednopodstawkowym (single-socket), min. 8 rdzeni fizycznych, min. 16 wątków logicznych; architektura 64-bitowa x86
2.2	Taktowanie bazowe min. 2,5 GHz, taktowanie Turbo min. 5,0 GHz
2.3	Cache LLC min. 16 MB
2.4	Obsługa instrukcji virtualizacji sprzętowej (VT-x) oraz virtualizacji We/Wy (VT-d)
2.5	TDP procesora nie wyższe niż 95 W
3.	Pamięć operacyjna RAM
3.1	Pamięć zainstalowana: min. 64 GB DDR5 ECC UDIMM
3.2	Taktowanie pamięci: min. 4400 MT/s
3.3	Konfiguracja modułów: 2× 32 GB UDIMM — co najmniej 2 sloty wolne (platforma posiada 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 hypervisor): dedykowany wewnętrzny moduł z dwoma dyskami M.2 NVMe o pojemności min. 480 GB każdy, skonfigurowanymi w RAID 1 — oddzielony fizycznie od przestrzeni danych maszyn wirtualnych; wymaga dedykowanego kontrolera boot (BOSS lub równoważny)
4.2	Warstwa danych produkcyjnych: cztery dyski SSD SATA 2,5" o pojemności min. 960 GB każdy, skonfigurowane w RAID 10 — minimalna pojemność netto ok. 1,9 TB; przeznaczone dla maszyn wirtualnych, bazy danych i systemu ERP
4.3	Warstwa danych pojemnościowych: dwa dyski HDD SATA 2,5" o pojemności min. 2,4 TB każdy, skonfigurowane w RAID 1 — minimalna pojemność netto ok. 2,4 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, z dedykowaną pamięcią podręczną (cache) min. 8 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
4.7	Obsługa szyfrowania danych na poziomie kontrolera (self-encrypting drives / controller-based encryption)
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
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 Możliwość centralnego zarządzania wieloma serwerami przez konsolę producenta dostępną przez przeglądarkę — obejmującą monitoring, aktualizację firmware i raportowanie bez konieczności logowania się do każdego serwera osobno
- 6.6 Obsługa SNMP v1–v3, SMTP (alerty e-mail), Syslog — do integracji z zewnętrznymi systemami monitoringu i SIEM
- 6.7 Port konsoli szeregowej (RS-232 lub USB) do lokalnego zarządzania awaryjnego
- 6.8 Możliwość zdalnej aktualizacji oprogramowania układowego (firmware) serwera i kontrolera BMC bez przerywania pracy serwera (gdzie technicznie możliwe)
7. Wirtualizacja i oprogramowanie
 - 7.1 Serwer musi być oficjalnie certyfikowany i figurować na liście zgodności (HCL) producenta wybranego hypervisora — co najmniej jednego z: VMware ESXi, Microsoft Hyper-V, Proxmox VE, Red Hat KVM
 - 7.2 Obsługa sprzętowej wirtualizacji We/Wy (SR-IOV) dla kart sieciowych
 - 7.3 Sprzętowy moduł TPM 2.0 wbudowany — wymagany dla bezpiecznego rozruchu hypervisora i szyfrowania woluminów maszyn wirtualnych
 - 7.4 Obsługa Secure Boot oraz sprzętowej weryfikacji integralności firmware (Silicon Root of Trust) przy każdym uruchomieniu serwera
8. Parametry wydajnościowe
 - 8.1 Przepustowość magistrali pamięci: min. 70 GB/s (DDR5 dual-channel)
 - 8.2 Obsługa PCIe 4.0 lub nowszego — min. jeden slot PCIe x8 lub x16 full-height dostępny na rozbudowę
 - 8.3 Obsługa min. 8 dysków 2,5" hot-plug w zatokach przednich oraz min. 2 slotów M.2 wewnętrznych przeznaczonych na moduł 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 (Silicon Root of Trust) — uniemożliwiająca uruchomienie serwera z zmodyfikowanym lub złośliwym firmware
 - 9.3 Obsługa szyfrowania dysków (SED — Self-Encrypting Drives) z zarządzaniem kluczami przez kontroler RAID lub zewnętrzny serwer kluczy zgodny ze standardem KMIP
 - 9.4 Czujnik otwarcia obudowy (intrusion detection switch) z alertem rejestrowanym w kontrolerze BMC i systemie zarządzania
10. Gwarancja i wsparcie
 - 10.1 Gwarancja producenta minimum 36 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 Rzeczypospolitej Polskiej; w przypadku braku własnego centrum serwisowego producenta w Polsce — oferent zobowiązany do przedłożenia dokumentu wskazującego autoryzowany podmiot serwisowy
 - 10.3 Możliwość rozszerzenia gwarancji do 60 miesięcy (5 lat) bez wymiany sprzętu
 - 10.4 Oświadczenie producenta lub autoryzowanego dystrybutora potwierdzające posiadanie przez oferenta autoryzacji w zakresie sprzedaży i serwisu oferowanych rozwiązań na terenie Polski

2. Serwer NAS

Parametr	Opis
Obudowa	Rack
Procesor	Czterordzeniowy procesor o taktowaniu 2,2 GHz osiągający w teście PassMark w lipcu 2022 co najmniej 4580 punktów
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 portu eSATA
Porty zewnętrzne	Minimum: <ul style="list-style-type: none">• 2 porty USB 3.2.1• 1 eSATA (jako gniazdo rozszerzenia)
Porty sieciowe	Minimum: <ul style="list-style-type: none">• 4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego)• karta sieciowa 10G zainstalowana w rozszerzeń PCIe x8

Funkcja Wake on LAN/WAN

Gniazdo rozszerzeń Min. 1x 4-liniowe gniazdo x8 PCIe 3.0

Wentylator obudowy Min. 2 wentylatory 80 mm x 80 mm

Obsługiwane protokoły sieciowe Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV

Obsługiwane systemy plików Min.:
• Wewnętrzny: Btrfs, ext4
Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT

Zarządzanie pamięcią masową
• Maksymalny rozmiar pojedynczego wolumenu: 108 TB
• Minimalny liczba wewnętrznych wolumenów: 64
• Minimalny liczba obiektów iSCSI Target: 128
• Minimalny liczba jednostek iSCSI LUN: 256
Obsługa klonowania/migawek jednostek iSCSI LUN

Dyski twarde
• Dedykowane dla macierzy 4 dyski HDD 7200 rpm, modele dedykowane dla NAS o wysokiej trwałości, wskazane na liście zgodności producenta NAS, 8 TB każdy

Obsługiwane macierzy RAID typy Min. SHR, Basic, 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/File Station 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®, Internet Explorer® 10 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, kompleksowe 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 Centrum Pakietów Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agentów na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików oprogramowania biurowego w czasie rzeczywistym.

Konserwacja Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwanych szyn rack

Zasilanie Wymogiem jest dostarczenie sprzętu wyposażonego w nadmiarowy zasilacz

Gwarancja	<ul style="list-style-type: none"> • 3 lata gwarancji producenta na serwer NAS. • 3 lata gwarancji na zainstalowane dyski twarde. • 1 rok na dodatkowe akcesoria montażowe w postaci przesuwanych szyn rack • Serwis ma być świadczony w miejscu instalacji urządzeń. • 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
Moc pozorna (VA)	Min. 3000 VA
Moc czynna (W)	Min. 2700 W (współczynnik mocy 0.9)
Topologia	Line-interactive z automatyczną regulacją napięcia (AVR)
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	6 x 12 V / 9 Ah, bezobsługowe, ołowiono-kwasowe (VRLA), wymienne przez użytkownika
Zarządzanie baterią	System ABM (Advanced Battery Management), ładowanie z kompensacją temperatury, 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	Min. 96% do 98% w trybie line-interactive, certyfikat ENERGY STAR
Interfejs użytkownika	Graficzny wyświetlacz LCD z obsługą wielu języków
Porty komunikacyjne	USB (HID), RS232, złącze przekaźnikowe (dry contact), złącze do zdalnego włączania/wyłączania, slot rozszerzeń (z kartą sieciową w zestawie)
Zarządzanie oprogramowaniem	i 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: 0–90% (bez kondensacji), wysokość: do 3000 m n.p.m.
Wymiary	Max. 770 mm (głębokość) x 430 mm (szerokość) x 86 mm (wysokość 2U)
Waga	Max. 33 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, kabel RS232, przewody IEC, instrukcja szybkiego startu, instrukcje bezpieczeństwa
Certyfikaty zgodność	i CE, RoHS, REACH, IEC/EN 62040-1/2/3, UL 1778, CSA 22.2, cTUVus, EAC, UKCA, ENERGY STAR
Gwarancja wsparcie techniczne	i Min. 3 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.
Szkolenie dokumentacja	i Wymagane przeszkolenie administratora (min. 1 godzina) z zakresu: konfiguracji i uruchomienia urządzenia, zarządzania zasilaniem i integracji z systemami IT, diagnostyki i reagowania na zdarzenia awaryjne, obsługi oprogramowania do zarządzania UPS. Szkolenie musi być przeprowadzone w języku polskim, w formie zdalnej lub stacjonarnej.

Wymagane jest również 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 virtualizacji

Lp.	Wymaganie
1.	Typ i architektura platformy virtualizacji
1.1	Platforma virtualizacji klasy Type 1 (hypervisor działający bezpośrednio na sprzęcie), wbudowana w środowisko serwerowego systemu operacyjnego — bez konieczności zakupu odrębnego oprogramowania hypervisora
1.2	Pełna obsługa maszyn wirtualnych generacji 2 (Gen 2) — opartych na firmware UEFI, z obsługą Secure Boot i wirtualnego modułu TPM (vTPM 2.0) dla każdej VM
1.3	Zarządzanie maszynami wirtualnymi możliwe z poziomu graficznego interfejsu zarządzczego (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 virtualizacji (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	Maksymalna liczba wirtualnych procesorów (vCPU) na maszynę wirtualną: 2 048 (dotyczy VM Gen 2)
3.2	Maksymalna ilość pamięci RAM na maszynę wirtualną: 240 TB (dotyczy VM Gen 2)
3.3	Obsługa pamięci dynamicznej (Dynamic Memory) — automatyczne dostosowywanie przydziału RAM do VM w zależności od bieżącego obciążenia
3.4	Maksymalna pojemność pojedynczego wirtualnego dysku twardego (VHDX): 64 TB
3.5	Obsługa do 256 dysków SCSI i 4 kontrolerów SCSI na maszynę wirtualną
3.6	Obsługa do 68 wirtualnych kart sieciowych na maszynę wirtualną
4.	Parametry skalowalności hosta
4.1	Maksymalna ilość pamięci RAM hosta obsługiwana przez platformę: 4 PB (przy procesorach obsługujących 5-poziomowe stronicowanie); przy 4-poziomowym stronicowaniu: 256 TB
4.2	Obsługa klastrowania hostów virtualizacji: klastry do 64 węzłów obsługujące łącznie do 8 000 maszyn wirtualnych
4.3	Obsługa klastrowania bezdomeny (Workgroup Cluster) — bez konieczności posiadania Active Directory, dedykowane dla środowisk brzegowych
5.	Sieć wirtualna i przełączniki
5.1	Wbudowany przełącznik wirtualny (Virtual Switch) obsługujący tryby: zewnętrzny, wewnętrzny i prywatny — umożliwiający izolację ruchu sieciowego VM
5.2	Obsługa akceleracji sieciowej SR-IOV (Single Root I/O Virtualization) — bezpośredni dostęp VM do fizycznej karty sieciowej z pominięciem warstwy hypervisora, minimalizacja opóźnień sieciowych
5.3	Obsługa virtualizacji sieciowej (NVGRE, VXLAN) do tworzenia izolowanych sieci wirtualnych między VM niezależnie od fizycznej topologii sieci
5.4	Obsługa Quality of Service (QoS) dla ruchu sieciowego VM — możliwość ograniczenia i gwarantowania przepustowości per VM lub per wirtualna karta sieciowa
6.	Bezpieczeństwo maszyn wirtualnych
6.1	Obsługa wirtualnego modułu TPM 2.0 (vTPM) dla każdej VM — umożliwia szyfrowanie dysku VM algorytmem BitLocker lub równoważnym bez dostępu do fizycznego TPM hosta
6.2	Obsługa Secure Boot dla maszyn wirtualnych Gen 2 — weryfikacja integralności bootloadera VM przed uruchomieniem
6.3	Obsługa Shielded VM (chronionych maszyn wirtualnych) — szyfrowanie stanu i konfiguracji VM uniemożliwiające odczyt danych przez administratora hosta
6.4	Izolacja środowisk maszyn wirtualnych — brak możliwości dostępu jednej VM do zasobów pamięci lub dysku innej VM bez jawnej zgody administratora

7. Wysoka dostępność i ciągłość działania

- 7.1 Obsługa migracji na żywo (Live Migration) — przenoszenie działającej VM między hostami bez przerwy w pracy i bez utraty połączeń sieciowych
- 7.2 Obsługa Quick Migration — szybka migracja VM przy minimalnym czasie przestoju (alternatywa dla Live Migration w środowiskach bez współdzielonego storage)
- 7.3 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)
- 7.4 Obsługa Storage Migration — przenoszenie plików VM (dysków VHDX) między lokalizacjami storage bez zatrzymywania VM
- 7.5 Obsługa replikacji VM do zapasowego hosta (Hyper-V Replica) — asynchroniczna replikacja danych VM do lokalizacji DR z konfigurowalnym interwałem (do 30 sekund)

8. Obsługiwane systemy operacyjne gości (VM)

- 8.1 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)
- 8.2 Obsługa usług integracji dla VM (Integration Services) zapewniających: synchronizację czasu, wymianę danych host–gość, spójny backup VSS, zamknięcie VM z hosta

9. Licencjonowanie — wymagania specyficzne dla edycji Standard systemu operacyjnego hosta

- 9.1 Platforma wirtualizacji musi być licencjonowana w modelu umożliwiającym uruchamianie maszyn wirtualnych z dedykowanym systemem operacyjnym — licencja obejmuje prawa do uruchamiania wirtualnych instancji systemu operacyjnego (OSE) na serwerze fizycznym
- 9.2 Licencja na platformę wirtualizacji oparta na rdzeniach fizycznego serwera (per core); minimalna liczba licencji rdzeniowych: 16 łącznie na serwer (min. 8 na procesor) — wszystkie rdzenie fizyczne serwera muszą być objęte licencją
- 9.3 Podstawowy zakres licencji obejmuje prawo do uruchamiania min. 2 wirtualnych instancji systemu operacyjnego (OSE) na w pełni zlicencjonowanym serwerze; możliwość rozszerzenia liczby licencjonowanych VM przez dokupienie dodatkowych pakietów licencji rdzeniowych (każdy pełny pakiet rdzeniowy = kolejne 2 VM z systemem operacyjnym)
- 9.4 Przy planowaniu 6–10 maszyn wirtualnych z systemem operacyjnym wymagane jest odpowiednie zwielokrotnienie licencji rdzeniowych lub zastosowanie edycji z nieograniczonymi prawami do wirtualizacji (Datacenter lub równoważna) — decyzja powinna być podjęta na etapie projektowania środowiska z uwzględnieniem całkowitego kosztu licencjonowania
- 9.5 Maszyny wirtualne uruchamiające systemy operacyjne inne niż objęte licencją hosta (np. Linux) nie wymagają dodatkowych licencji w ramach platformy wirtualizacji — brak ograniczenia liczby takich VM
- 9.6 Host fizyczny z uruchomioną platformą wirtualizacji może równolegle uruchamiać oprogramowanie infrastrukturalne (backup, monitoring, narzędzia zarządzania) bez zużywania praw do licencjonowanych wirtualnych OSE — pod warunkiem że host nie jest używany do uruchamiania aplikacji biznesowych niezwiązanych z zarządzaniem wirtualizacją
- 9.7 Licencje dostępu klienta (CAL) są wymagane dla każdego użytkownika lub urządzenia uzyskującego dostęp do usług systemu operacyjnego działającego na platformie wirtualizacji (zarówno na hoście, jak i w maszynach wirtualnych); CAL muszą odpowiadać wersji zainstalowanego systemu operacyjnego

10. Zarządzanie i monitorowanie

- 10.1 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
- 10.2 Obsługa automatyzacji i skryptowania przez wbudowany interfejs wiersza poleceń (PowerShell) — pełen zestaw poleceń cmdlet do zarządzania VM, switchami wirtualnymi, dyskami i migracją
- 10.3 Obsługa protokołu WMI/CIM do integracji z zewnętrznymi systemami monitoringu i zarządzania (SCCM, SCOM lub równoważne)
- 10.4 Wbudowane narzędzia do monitorowania wydajności VM i hosta: Menedżer zasobów, liczniki wydajności dostępne przez narzędzia monitoringu systemu operacyjnego

Wymagania licencyjne platformy wirtualizacji

Parametr	Opis wymagań funkcjonalnych
Typ licencji	Licencja dołączana do systemu operacyjnego klasy serwerowej, przeznaczona do środowisk fizycznych lub zwirtualizowanych.
Instalacja na fizycznym	Instalacja na hoście. Licencja musi umożliwiać instalację systemu operacyjnego bezpośrednio na fizycznym serwerze.
Wirtualizacja	Licencja musi umożliwiać jednoczesne uruchomienie co najmniej dwóch instancji systemu operacyjnego jako maszyn wirtualnych na tym samym hoście fizycznym.
Hypervisor	System operacyjny musi zawierać wbudowaną rolę hipernadzorcy (hypervisora) umożliwiającą zarządzanie maszynami wirtualnymi bez konieczności instalacji dodatkowego oprogramowania.

Konteneryzacja	Brak ograniczeń co do liczby uruchamianych kontenerów systemowych oraz możliwość uruchamiania kontenerów izolowanych (np. z własnym jądrem).
Model licencjonowania	Licencjonowanie oparte na liczbie fizycznych rdzeni procesora zainstalowanych w serwerze.
Licencje dostępne (CAL)	Wymagana zgodność z aktualnymi zasadami licencjonowania środowisk serwerowych, w tym konieczność posiadania licencji dostępnych (CAL) dla użytkowników lub urządzeń uzyskujących dostęp do usług serwera.
Aktualność	Licencja musi odpowiadać funkcjonalnościom oferowanym w aktualnej wersji systemu operacyjnego klasy serwerowej dostępnej na rynku w roku 2025.

5. System Operacyjny Serwera (2 sztuki)

Lp. Wymaganie	
1.	Wersja i cykl życia
1.1	Serwerowy system operacyjny w najnowszej dostępnej wersji z kanału Long-Term Servicing Channel (LTSC) — gwarantującego stabilność i długoterminowe wsparcie bez narzuconych aktualizacji funkcjonalnych, dostarczony wraz z serwerem.
1.2	Wsparcie główne (Mainstream Support): min. do 2029 roku; wsparcie rozszerzone (Extended Support): min. do 2034 roku — łącznie min. 10 lat wsparcia od daty premiery
1.3	Edycja Standard — dedykowana środowiskom z niską lub umiarkowaną gęstością wirtualizacji; obejmuje wbudowaną platformę wirtualizacji (Type 1 hypervisor) zgodnie z wymaganiami określonymi w odrębnej specyfikacji platformy wirtualizacji
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, rzuty 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 SATA/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, Credential Guard i Secured-Core Server
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 (Active Directory Domain Services — AD DS) umożliwiająca centralne zarządzanie kontami użytkowników, komputerów, grup i polityk bezpieczeństwa w domenie
3.2	Obsługa nowych poziomów funkcjonalności domeny i lasu (DomainLevel 10, ForestLevel 10) odblokowujących zaawansowane funkcje usług katalogowych
3.3	Baza danych usług katalogowych ze zwiększonym rozmiarem strony do 32 KB (wzrost z 8 KB) — lepsza skalowalność obiektów i atrybutów katalogu
3.4	Obsługa delegowanych kont usług zarządzanych (dMSA — Delegated Managed Service Accounts) — automatyczne zarządzanie hasłami kont usługowych bez konieczności ręcznej rotacji
3.5	Wbudowane rozwiązanie do zarządzania hasłami lokalnych administratorów (LAPS) — automatyczne generowanie i rotacja unikalnych haseł lokalnych kont administracyjnych z przechowywaniem w usłudze katalogowej
3.6	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 SMB over QUIC — bezpieczny dostęp do zasobów plikowych przez sieci niezaufane z szyfrowaniem TLS bez konieczności stosowania VPN; dostępne w edycji Standard
- 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 pulpitu; 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 Secured-Core Server — wielowarstwowa ochrona sprzętowa i firmware'owa obejmująca: Secure Boot, sprzętową izolację oprogramowania DRTM (Dynamic Root of Trust for Measurement), ochronę HVPT (Hypervisor-Protected Page Tables) oraz izolację sterowników
- 5.2 Credential Guard — domyślnie włączony na wspierającym sprzęcie; izolacja danych uwierzytelniających w sprzętowym kontenerze opartym o virtualizację (VBS), ochrona przed atakami Pass-the-Hash i kradzieżą tokenów
- 5.3 Szyfrowanie dysków systemowych i danych algorytmem BitLocker z kluczem zarządzanym przez TPM 2.0; obsługa automatycznego odblokowywania woluminów danych
- 5.4 Domyślne szyfrowanie LDAP (LDAP over TLS 1.3) dla wszystkich połączeń do usługi katalogowej — ochrona danych katalogowych w transmisji
- 5.5 Wbudowany mechanizm zarządzania politykami bezpieczeństwa (Group Policy) — centralnie dystrybuowane i wymuszane ustawienia bezpieczeństwa dla wszystkich stacji roboczych i serwerów w domenie
- 5.6 Gotowy profil zabezpieczeń (Security Baseline) z ponad 350 skonfigurowanymi ustawieniami bezpieczeństwa zgodnymi z rekomendacjami branżowymi — możliwość stosowania od momentu instalacji
- 5.7 Wirtualizacyjne enklawy bezpieczeństwa (VBS Enclaves) — izolacja wrażliwych procesów i danych od pozostałej części systemu i hosta wirtualizacji
- 6. Zarządzanie i automatyzacja
- 6.1 Graficzna konsola zarządzania serwerem (Server Manager lub równoważna) 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 (PowerShell) z pełnym zestawem poleceń cmdlet do automatyzacji zadań administracyjnych, zarządzania rolami, politykami i infrastrukturą wirtualizacji
- 6.4 Wbudowany terminal wieloprofilowy (Windows Terminal) z obsługą PowerShell, CMD i SSH w jednym interfejsie
- 6.5 Wbudowane narzędzie diagnostyczne DTrace do monitorowania i analizy wydajności systemu w czasie rzeczywistym bez konieczności instalowania zewnętrznych narzędzi
- 6.6 Obsługa protokołu SNMP (v1–v3) oraz WMI/CIM do integracji z zewnętrznymi systemami monitoringu i zarządzania infrastrukturą
- 7. Aktualizacje i patching
- 7.1 Obsługa aktualizacji bezpieczeństwa bez restartu serwera (Hotpatching) — dostępna dla maszyn wirtualnych połączonych z platformą chmury hybrydowej (Azure Arc); minimalizacja przestoju podczas aktualizacji środowisk produkcyjnych
- 7.2 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
- 7.3 Możliwość zakupu licencji w modelu jednorazowym (licencja wieczysta) lub subskrypcyjnym (pay-as-you-go poprzez integrację z chmurą hybrydową)
- 8. Wydajność i pamięć masowa
- 8.1 Zoptymalizowana obsługa dysków NVMe — wzrost przepustowości operacji We/Wy (IOPS) o min. 60% w porównaniu do poprzedniej wersji systemu przy identycznym sprzęcie
- 8.2 Obsługa systemu plików ReFS z funkcją Block Cloning — przyspieszone kopiowanie plików z poprawą wydajności do 90% dla operacji na dużych plikach
- 8.3 Obsługa replikacji danych Storage Replica między serwerami lub klastrem z kompresją danych przesyłanych przez sieć — redukcja zużycia pasma podczas replikacji; w edycji Standard: jedno partnerstwo replikacji i jedna grupa zasobów
- 8.4 Obsługa akceleracji sieciowej SR-IOV (AcceNet) 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 Model licencjonowania oparty na rdzeniach fizycznych (per core); minimalna liczba licencji: 16 rdzeni na serwer (min. 8 na procesor); licencje sprzedawane w pakietach 2-rdzeniowych i 16-rdzeniowych

- 9.2 Edycja Standard obejmuje prawa do uruchamiania 2 wirtualnych instancji serwerowego systemu operacyjnego na w pełni zlicencjonowanym serwerze; każde kolejne 2 VM z serwerowym systemem operacyjnym wymagają pełnego zestawu licencji rdzeniowych dla serwera (stacking); brak limitu dla VM z innymi systemami operacyjnymi (np. Linux)
- 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 (40 sztuk)

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 Licencja CAL jest wymagana nawet w przypadku dostępu pośredniego (multiplexing) — agregowanie połączeń przez oprogramowanie pośredniczące nie eliminuje obowiązku posiadania CAL dla użytkowników końcowych
- 1.3 Licencje CAL nie są sprawdzane technicznie przez system operacyjny serwera — są wymagane prawnie i podlegają weryfikacji podczas audytów licencyjnych; zamawiający ponosi odpowiedzialność za właściwe ich udokumentowanie i ewidencję
- 1.4 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)
- 1.5 Dostęp anonimowy do publicznie dostępnych usług webowych (publiczna strona WWW bez uwierzytelniania) oraz usług DHCP i DNS nie wymaga licencji CAL

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 posiadają prawo do downgrade — umożliwiają dostęp do serwerów ze starszymi wersjami systemu operacyjnego (co najmniej 3 generacje wstecz) bez konieczności zakupu oddzielnych licencji dla starszych serwerów
- 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)
- 3.3 Wybór między CAL per użytkownik a CAL per urządzenie należy do zamawiającego i powinien być oparty na analizie środowiska — dopuszczalne jest stosowanie obu typów jednocześnie w tej samej organizacji (np. CAL per użytkownik dla pracowników biurowych, CAL per urządzenie dla stanowisk współdzielonych)
- 3.4 Dla zewnętrznych użytkowników (klientów, partnerów, kontrahentów spoza organizacji) alternatywą dla indywidualnych CAL jest licencja zbiorowa External Connector — przypisywana do serwera i uprawniająca do nieograniczonego dostępu zewnętrznych użytkowników do tego serwera

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 zależy od modelu pracy użytkowników
- 4.3 RDS CAL musi odpowiadać wersji serwera pełniącego rolę hosta sesji pulpitu zdalnego (RD Session Host) — licencje RDS CAL dla wcześniejszych wersji nie uprawniają do dostępu do nowszych wersji RD Session Host; dostępne jest prawo do downgrade (nowsza RDS CAL → starszy RD Session Host)
- 4.4 W środowisku z usługami pulpitu zdalnego wymagany jest dedykowany serwer licencji RDS (RD Licensing Server) do wydawania i śledzenia licencji RDS CAL; może to być ta sama maszyna co RD Session Host lub osobna VM
- 4.5 Okres próbny (grace period) dla RDS: 120 dni od momentu uruchomienia roli RD Session Host bez zainstalowanych licencji RDS CAL — po tym czasie serwer odmówi połączeń zdalnych; licencje RDS CAL należy zainstalować przed upływem okresu próbnego
- 4.6 Standardowy CAL dostępu do serwera (pkt 3.1–3.3) nie zastępuje RDS CAL — oba rodzaje licencji są wymagane łącznie przy korzystaniu z usług pulpitu zdalnego

5. Ilość licencji wymaganych w zamówieniu

- 5.1 Liczba licencji CAL musi odpowiadać łącznej liczbie użytkowników lub urządzeń uzyskujących dostęp do usług serwerowych w organizacji; zamawiający określa wymaganą liczbę na podstawie aktualnego stanu zatrudnienia i planowanego rozwoju
- 5.2 Liczba licencji RDS CAL musi odpowiadać liczbie użytkowników lub urządzeń korzystających z usług pulpitu zdalnego — może być mniejsza niż łączna liczba CAL, jeśli nie wszyscy użytkownicy korzystają z usług zdalnego pulpitu
- 5.3 Licencje CAL i RDS CAL są sprzedawane w pakietach (np. 1, 5, 10, 20, 50 sztuk) — ilość w zamówieniu powinna odpowiadać rzeczywistemu zapotrzebowaniu z uwzględnieniem marginesu na nowych pracowników w okresie obowiązywania kontraktu

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. 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) Realizacja przedmiotu zamówienia odbywać się będzie zdalnie oraz lokalnie w zakresie właściwym dla zadania. Realizacja zleconych zadań może wymagać w uzasadnionych przypadkach obecności Wykonawcy w siedzibie Zamawiających nawet jeżeli określono realizację zdalną wybranego zakresu, jeżeli zdalna realizacja będzie niemożliwa lub może negatywnie wpływać na jakość wykonania przedmiotu projektu.
- c) Wykonawca musi przekazywać w trakcie realizacji czynności przewidzianych niniejszym zamówieniem informacje o wszelkich wykrytych podatnościach, w celu umożliwienia Zamawiającemu podjęcia natychmiastowych działań naprawczych.
- d) Wykonawca każdorazowo, winien uzgadniać z Zamawiającym termin prowadzenia bardziej inwazyjnych czynności ze szczególnym uwzględnieniem: DoS, i prowadzić je dopiero po uzyskaniu pisemnej, w tym poprzez środki elektronicznej komunikacji, zgody osoby Zamawiającego. Wykonawca musi prowadzić prace, które umożliwią mu zakończenie w każdym momencie takich testów.
- e) Jakiegokolwiek czynności prowadzone przez Wykonawcę nie mogą spowodować przestoju w świadczeniu usług przez Zamawiającego. Gdyby jednak przeprowadzenie testów rodziło ryzyko przestoju w pracy, Wykonawca w porozumieniu z Zamawiającym Wykonawcą opracuje, zaakceptowany przez Zamawiającego, scenariusz alternatywny przeprowadzenia testów tak aby zminimalizować ryzyko problemów.
- f) Wykonawca może prowadzić prace po uprzednim uzgodnieniu ich zakresu z każdym z Zamawiających. Przez uzgodnienie należy rozumieć precyzyjne wskazanie daty oraz czasu rozpoczęcia a także zakończenia prac.
- g) Wykonawca ma obowiązek ścisłej współpracy z Zamawiającym na każdym etapie realizacji zamówienia.
- h) Wykonawca winien uwzględniać wszelkie uwagi Zamawiającego, które doprecyzowują lub uzupełniają zapisy w zapytaniu ofertowym i nie są z nimi sprzeczne.
- i) Zamawiający we współpracy z Wykonawcą ustalą harmonogram spotkań mających na celu weryfikację stanu projektu. Zakłada się minimalną częstotliwość spotkań raz w tygodniu.
- j) Wykonawca musi dostosować się do polityk bezpieczeństwa Zamawiającego.
- k) W niniejszym dokumencie opisano wymagania minimalne.

8. Wdrożenie

- a) Każdy z systemów stanowiący przedmiot dostawy winien zostać wdrożony w sposób umożliwiający prawidłowe funkcjonowanie bez negatywnego wpływu na środowisko Zamawiającego.
- b) W przypadku dostawy licencji Wykonawca wdroży minimalnie 20% licencji oraz skonfiguruje całość rozwiązania by działało prawidłowo.
- c) Zakres funkcjonalny związany z domeną AD, musi zostać wdrożony przez wykonawcę w min. 80 % (na urządzeniach zamawiającego)
- d) W przypadku dostawy rozwiązania opierającego się o serwer Wykonawca wdroży je w całości na serwerze oraz w 20% na urządzeniach/użytkownikach objętych wdrożeniem.
- e) Wdrożenie ma odbywać się wraz z Zamawiającym co oznacza, że Wykonawca będzie prowadził prace bezpośrednio w obecności Zamawiającego.