Załącznik Nr 1a do SWZ

Szczegółowy opis przedmiotu zamówienia dla części I

Zakup oraz dostawa serwerów wraz z oprogramowaniem

1) Zamówienie dla Urzędu Miasta Mława

1. Serwer z oprogramowaniem – 1 sztuka

Specyfikacje minimalnych wymagań:

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Obudowa Rack o wysokości max 1U z możliwością instalacji 8 dysków 2.5” • Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze.
Płyta główna	• Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Płyta powinna obsługiwać do min. 128GB, na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone dla pamięci
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych
Procesor	Jeden procesor Minimum 8 rdzeni fizycznych. Minimum 16 wątków logicznych (obsługa technologii wielowątkowości/Hyper-Threading). Bazowa częstotliwość taktowania procesora nie mniejsza niż 3,2 GHz.

	Maksymalna częstotliwość Turbo nie niższa niż 5,6 GHz. Pamięć podręczna trzeciego poziomu (L3) nie mniejsza niż 24 MB. Obsługa pamięci typu DDR5 Współczynnik TDP nie większy niż 95 W. Wynik nie mniejszy niż 95.1 punktów w teście SPECrate2017_int_base (w konfiguracji jednoprocesorowej), zgodnie z danymi opublikowanymi na stronie: https://www.spec.org. Wynik nie mniejszy niż 28 974 punktów w teście PassMark CPU Mark, zgodnie z danymi zawartymi na stronie: https://www.cpubenchmark.net.
Pamięć RAM	• 4x32GB pamięci RAM DDR5 UDIMM o częstotliwości pracy 4800MT/s.
Kontroler RAID	• Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID: 0, 1, 10
Dyski twarde	• Zainstalowane ○ 2x dysk SAS o pojemności min. 1.2TB, Hot-Plug. • Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
Sloty PCIe	• Dwa sloty PCIe
Interfejsy sieciowe/FC/SAS	• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT

Wbudowane porty	• min. 4 porty USB w tym min:
	  ○ 1 port USB 3.0 z tyłu obudowy,
	  ○ 1 port micro USB z przodu obudowy
	• 1 port VGA na tylnym panelu,
	• 1 port RS232

Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
Zasilacze	2 szt. redundantne, o mocy maks. 700W klasy Titanium
Elementy montażowe	Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych
Wymagania	**Serwer musi być kompatybilny z poniżej podaną specyfikacją macierzy dyskowej.**
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 V3 • Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).

Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: o zdalny dostęp do graficznego interfejsu Web karty zarządzającej; o zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); o szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; o możliwość podmontowania zdalnych wirtualnych napędów; o wirtualną konsolę z dostępem do myszy, klawiatury; o wsparcie dla IPv6; o wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; o możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; o możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; o integracja z Active Directory; o możliwość obsługi przez dwóch administratorów jednocześnie; o wsparcie dla dynamic DNS; o wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. o możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera o możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: o Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej o Przesyłanie danych telemetrycznych w czasie rzeczywistym o Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze o Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: o Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych o integracja z Active Directory o Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta o Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish o Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram o Szczegółowy opis wykrytych systemów oraz ich komponentów o Możliwość eksportu raportu do CSV, HTML, XLS, PDF o Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. o Grupowanie urządzeń w oparciu o kryteria użytkownika o Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji o Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach o Szybki podgląd stanu środowiska o Podsumowanie stanu dla każdego urządzenia

	○ Szczegółowy status urządzenia/elementu/komponentu ○ Generowanie alertów przy zmianie stanu urządzenia. ○ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń ○ Integracja z service desk producenta dostarczonej platformy sprzętowej ○ Możliwość przejęcia zdalnego pulpitu ○ Możliwość podmontowania wirtualnego napędu ○ Kreator umożliwiający dostosowanie akcji dla wybranych alertów ○ Możliwość importu plików MIB ○ Przesyłanie alertów „as-is" do innych konsol firm trzecich ○ Możliwość definiowania ról administratorów ○ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów ○ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) ○ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta ○ Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów ○ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. ○ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. ○ Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile ○ Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. ○ Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. ○ Zdalne uruchamianie diagnostyki serwera. ○ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. ○ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT **oraz integrację z posiadaną przez Zamawiającego platformą wirtualizacji Vmware (lub kompatybilną).** Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: • Monitoring: ○ ilość podłączonych oraz rozłączonych systemów ○ stan podłączonych urządzeń ○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów ○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia ○ informacje o statusie gwarancji dla poszczególnych urządzeń

	○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń ○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. ○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych ○ Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. ○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. ○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. ○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. ○ Monitoring parametrów serwerów z informacją o minimum: ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ○ Monitoring parametrów pamięci masowych z informacją o minimum: ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów ○ Monitoring parametrów przełączników sieciowych z informacją o minimum: ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ▪ Stanie komponentów: zasilacze, wentylatory ▪ Podłączonych hostach ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów

- Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.

- Aktualizacja firmware
  - możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania
  - możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania
  - możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania
  - możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania
  - możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania
- Raporty
  - Możliwość generowania raportów dla serwerów zawierających informację o:
    - Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej
    - Średnim obciążeniu: procesorów, pamięci RAM, IO,
  - Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o:
    - Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji
  - Generowanie raportów do plików CSV i PDF
- Cyberbezpieczeństwo
  - Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia.
  - Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń.
  - Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.
  - Możliwość przypisania dedykowanych ról dla poszczególnych administratorów.
- Wspierane urządzenia
  - Urządzenie Producenta dostarczane w ramach postępowania
  - Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego)
- Wirtualny asystent

	○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne ○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android • Certyfikaty Oferowana platforma musi być zaprojektowana zgodnie z zasadami zarządzania bezpieczeństwem informacji, co najmniej równoważnymi normie ISO/IEC 27001. Za równoważne uznaje się m.in. zgodność ze standardami: • NIST SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations), • CSA Cloud Controls Matrix (CCM), lub innymi równoważnymi normami spełniającymi analogiczne wymagania dotyczące poufności, integralności i dostępności informacji.
Certyfikaty	• Producent oferowanego serwera musi posiadać wdrożony system zarządzania jakością zgodny z normą ISO 9001:2015 lub równoważną oraz systemy zarządzania środowiskowego i energetycznego zgodne z normami ISO 14001 i ISO 50001 lub równoważnymi. • Serwer musi posiadać deklarację zgodności **CE** lub równoważny potwierdzający dopuszczenie sprzętu do obrotu w Europejskim Obszarze Gospodarczym. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku lub równoważnego certyfikatu środowiskowego potwierdzającego spełnienie porównywalnych wymagań dotyczących efektywności energetycznej, zawartości substancji niebezpiecznych, recyklingu i trwałości produktu - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.**

	• Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2025.
Dokumentacja użytkownika	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Oprogramowanie serwerowe	**Oprogramowanie serwerowe – 2 sztuki** Wymagane minimalne parametry: System operacyjny Windows Server 2025 Standard (licencja na 16 rdzeni procesora, wersja OEM) lub równoważnego wraz z 28 pakietami licencji dostępów klienckich (CAL) typu User lub równoważnego. Opis równoważności dla systemu Windows Server 2025 Standard: 1. System operacyjny musi być przeznaczony do zastosowań serwerowych w Środowiskach fizycznych lub o minimalnej wirtualizacji. 2. System operacyjny musi być najnowszą wersją rodziny systemów operacyjnych danego producenta. 3. Licencja na system operacyjny musi uwzględniać prawo do bezpłatnej instalacji udostępnianych przez producenta poprawek krytycznych i opcjonalnych do zakupionej wersji oprogramowania co najmniej przez 5 lat. 4. Licencja na system operacyjny musi umożliwiać uruchomienie kontrolera domeny będącego w pełni zgodnym z domeną wdrożoną u Zamawiającego domeną Active Directory pracującą w oparciu o system Windows Server 2012 musi także być dostarczona możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server 5. Licencja na system operacyjny musi być bez ograniczeń czasowych. 6. Licencja na system operacyjny musi uprawniać do uruchamiania systemu operacyjnego w środowisku fizycznym i min. 2 środowiskach wirtualnych za pomocą wbudowanych mechanizmów wirtualizacji, bez konieczności zakupu dodatkowych licencji. 7. Zaimplementowanie w systemie operacyjnym środowiska wirtualizacyjnego musi umożliwiać dodawanie i usuwanie pamięci wirtualnej oraz wirtualnych kart sieciowych podczas pracy maszyny wirtualnej. 8. System operacyjny musi posiadać graficzny interfejs użytkownika. 9. System operacyjny musi być w pełni kompatybilny z usługą Active Directory w zakresie: a. zarządzania użytkownikami, b. zarządzania certyfikatami dla użytkowników wraz ze wsparciem możliwości logowania do domeny kartą mikroprocesorową, c. możliwości przydzielania praw dostępu do zasobów sieciowych, d. instalacji zdalnej oprogramowania z pakietów msi, e. definiowanie polityk bezpieczeństwa dla użytkowników, grup oraz stacji roboczych z systemami MS Windows: 7,8,8.1, 10,11. 10. System operacyjny musi wspierać pracę domenową wraz z automatyczną synchronizacją dla dodatkowych serwerów.

	11. System operacyjny musi posiadać obsługę zdalnego pulpitu poprzez protokół RDP. 12. System operacyjny musi umożliwiać ustawianie relacji zaufania pomiędzy domenami. 13. Wszystkie narzędzia i usługi systemu operacyjnego powinny być rozwiązaniem jednego producenta. 14. System operacyjny musi posiadać obsługę pamięci USB jako monitora klastra 15. System operacyjny musi pozwalać na stopniowe uaktualnienia systemu operacyjnego klastra 16. System operacyjny musi posiadać obsługę deduplikacji na potrzeby systemu plików ReFS. 17. System operacyjny musi posiadać obsługę optymalizacji transportu w tle pod kątem opóźnień. 18. System operacyjny musi posiadać wbudowaną zaporę internetową (firewall) dla ochrony połączeń internetowych; zapora musi być zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6; 19. System operacyjny musi posiadać możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny; 20. System operacyjny musi posiadać możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu; 21. System operacyjny musi posiadać obsługa PowerShelI 5.1, 22. System operacyjny musi posiadać obsługa certyfikatów w Active Directory 23. Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte muszą być dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).
Dodatkowe oprogramowanie serwerowe	**Dodatkowe oprogramowanie serwerowe 28 pakietów licencji dostępów klienckich (CAL) typu User lub równoważnego.** Licencje dostępowe typu Windows Server 2025 User CAL, a. w łącznej liczbie **140 sztuk,** b. w postaci 28 pakietów po 5 licencji (5-pack), c. wersja: Windows Server CAL 2025 Polish 1pk DSP OEI 5 Clt User CAL, licencje wieczyste, przypisane do użytkownika (User CAL).
Dodatkowe oprogramowanie serwerowe	**Oprogramowanie do wirtualizacji serwerów – 2 sztuki.** **1. Przedmiot zamówienia** Dostawa licencji czasowej na oprogramowanie do wirtualizacji infrastruktury serwerowej klasy enterprise, umożliwiającego zarządzanie maszynami wirtualnymi, obsługę środowiska wysokiej dostępności oraz migrację maszyn wirtualnych bez przestoju. **2. Wymagania licencyjne** Licencja przeznaczona na 1 fizyczny procesor (socket) o maksymalnie 16 rdzeniach. W przypadku procesora o większej liczbie rdzeni należy przewidzieć możliwość zakupu dodatkowych jednostek licencyjnych. Licencja czasowa na okres **do 25.03.2026 r.** Licencja powinna obejmować wyłącznie komponent programowy.

	Zamawiający wymaga dostawy 2 sztuk licencji czasowych (12 miesięcy) na oprogramowanie do wirtualizacji klasy enterprise, obejmujących po jednym fizycznym procesorze (socket) o maksymalnie 16 rdzeniach każdy. Środowisko docelowe składa się z dwóch serwerów jednoprocesorowych wyposażonych w procesory z 8 rdzeniami fizycznymi – z wynikiem nie mniejszym niż 28 974 punktów w teście PassMark CPU Mark, zgodnie z danymi zawartymi na stronie: https://www.cpubenchmark.net. **3. Wymagane funkcjonalności** Możliwość wirtualizacji maszyn x86_64. Centralne zarządzanie infrastrukturą wirtualną z poziomu dedykowanego kontrolera. Obsługa maszyn wirtualnych z różnymi systemami operacyjnymi (np. Linux, Windows). Migracja maszyn wirtualnych „na żywo" (bez przerywania ich pracy). Wysoka dostępność usług (automatyczne uruchamianie maszyn po awarii hosta fizycznego). Obsługa pamięci masowej lokalnej oraz sieciowej (m.in. NAS, SAN, NFS, iSCSI). Obsługa sieci VLAN, wirtualnych przełączników oraz segmentacji sieciowej. Graficzny interfejs zarządzania dostępny przez przeglądarkę internetową (HTML5). Możliwość planowania harmonogramów uruchamiania i wyłączania maszyn wirtualnych. Integracja z rozwiązaniami do wykonywania kopii zapasowych oraz systemami odtwarzania awaryjnego (Disaster Recovery). Obsługa środowisk klastrowych oraz rozproszonego zarządzania zasobami. Możliwość aktualizacji platformy bez przerywania pracy maszyn wirtualnych. **4. Wymagania techniczne** Oprogramowanie powinno być instalowane bezpośrednio na fizycznym sprzęcie serwerowym (bare-metal). Obsługa hostów fizycznych z architekturą x86_64. Obsługa minimum 128 GB RAM na hosta. Kompatybilność z rozwiązaniami do zarządzania infrastrukturą IT oraz backupem (np. poprzez API lub zewnętrzne integracje). Możliwość wdrożenia komponentu zarządzającego w postaci maszyny wirtualnej lub appliance. Możliwość współpracy z innym środowiskiem tego samego typu w ramach klastra, replikacji lub odtwarzania awaryjnego. Ugruntowana pozycja na rynku rozwiązań do wirtualizacji klasy enterprise. Długoletnie wsparcie techniczne producenta oraz dostępność dokumentacji. Stabilność i dojrzałość rozwiązania potwierdzona w zastosowaniach produkcyjnych. Integracja z rozwiązaniami do kopii zapasowych oraz rozwiązaniami do orkiestracji disaster recovery. Zgodność z normami bezpieczeństwa obowiązującymi w sektorze publicznym i finansowym. **5. Wyróżniki wymaganej platformy** • Dostarczone oprogramowanie musi być fabrycznie nowe, nieużywane, niewycofane z produkcji i pochodzić z legalnego, polskiego kanału dystrybucji.

	• Całość dostarczanego oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów na teren Polski – ze względów gwarancyjnych niedopuszczalne jest dostarczanie oprogramowania z tzw. brokerki, • Całość dostarczonego oprogramowania musi być ze sobą kompatybilna, Zamawiający uzyska dostęp do stron internetowych producentów rozwiązań, umożliwiający: • bezpłatne pobieranie najnowszego oprogramowania aktualizującego system do najnowszej wersji przez okres trwania licencji, • dostęp do dokumentacji sprzętu i oprogramowania, • dostęp do pomocy technicznej producenta.
Macierz dyskowa - 1 sztuka.	**Wymagania minimalne**
Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19”, o wysokość maksymalnie 2U z możliwością instalacji min. 24 dysków 2.5”
Przestrzeń dyskowa	Zainstalowane: 12x dysk SAS o pojemności min. 1.2TB, Hot-Plug
Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 240 dysków twardych.
Obsługa dysków	Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” jak również 3,5”.
Sposób zabezpieczenia danych	Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping). Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku). Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.
Tryb pracy kontrolerów macierzowych	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.

Pamięć cache	Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.
Rozbudowa pamięci cache	Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.
Interfejsy	Macierz musi posiadać, co najmniej 8 portów 12Gb SAS (4 porty na kontroler)
Kable/wkładki	8x kabel 12Gb HD Mini-SAS/HD Mini-SAS min. 2m
Zarządzanie	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.
Zarządzanie grupami dyskowymi oraz dyskami logicznymi	Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Thin Provisioning	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP). Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Tiering	Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS. Tiering musi obejmować wszystkie woluminy w danej puli dyskowej. Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.

Wewnętrzne kopie migawkowe	Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Wewnętrzne kopie pełne	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Migracja danych w obrębie macierzy	Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
Podłączanie zewnętrznych systemów operacyjnych	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.
Redundancja	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.

	Zasilacze użyte w macierzy powinny spełniać wymagania dotyczące sprawności dla zasilacza minimum 80+ Gold.
Dodatkowe wymagania	Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych. Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.
Standardy bezpieczeństwa	Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union), IEC 60950-1 (International)
Adaptery	3 szt. adapterów do podłączenia macierzy do obecnie funkcjonujących serwerów Dell Power Edge R350; R730; R750;
Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.
Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji systemów operacyjnych. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: • Monitoring: o ilość podłączonych oraz rozłączonych systemów o stan podłączonych urządzeń o informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów o Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia o informacje o statusie gwarancji dla poszczególnych urządzeń o informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń o informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. o Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych o Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych.

	○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. ○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. ○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. ○ Monitoring parametrów serwerów z informacją o minimum: ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ○ Monitoring parametrów pamięci masowych z informacją o minimum: ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów ○ Monitoring parametrów przełączników sieciowych z informacją o minimum: ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ▪ Stanie komponentów: zasilacze, wentylatory ▪ Podłączonych hostach ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Aktualizacja firmware ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania

	○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty ○ Możliwość generowania raportów dla serwerów zawierających informację o: ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, ○ Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji ○ Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo ○ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. ○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. ○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. ○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia ○ Urządzenie Producenta dostarczane w ramach postępowania ○ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) • Wirtualny asystent ○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne

	○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android • Certyfikaty Oferowana platforma musi być zaprojektowana zgodnie z zasadami zarządzania bezpieczeństwem informacji, co najmniej równoważnymi normie ISO/IEC 27001. Za równoważne uznaje się m.in. zgodność ze standardami: • NIST SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations), • CSA Cloud Controls Matrix (CCM), lub innymi równoważnymi normami spełniającymi analogiczne wymagania dotyczące poufności, integralności i dostępności informacji.

2. Oprogramowanie serwerowe System operacyjny Windows Server 2025 Standard lub równoważny – 2 sztuki

Oprogramowanie serwerowe	Wymagane minimalne parametry: System operacyjny Windows Server 2025 Standard (licencja na 16 rdzeni procesora) lub równoważny. Opis równoważności dla systemu Windows Server 2025 Standard: 1. System operacyjny musi być przeznaczony do zastosowań serwerowych w środowiskach fizycznych lub o minimalnej wirtualizacji. 2. System operacyjny musi być najnowszą wersją rodziny systemów operacyjnych danego producenta. 3. Licencja na system operacyjny musi uwzględniać prawo do bezpłatnej instalacji udostępnianych przez producenta poprawek krytycznych i opcjonalnych do zakupionej wersji oprogramowania co najmniej przez 5 lat. 4. Licencja na system operacyjny musi umożliwiać uruchomienie kontrolera domeny będącego w pełni zgodnym z domeną wdrożoną u Zamawiającego domeną Active Directory pracującą w oparciu o system Windows Server 2012 musi także być dostarczona możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server 5. Licencja na system operacyjny musi być bez ograniczeń czasowych. 6. Licencja na system operacyjny musi uprawniać do uruchamiania systemu operacyjnego w środowisku fizycznym i min. 2 środowiskach wirtualnych za pomocą wbudowanych mechanizmów wirtualizacji, bez konieczności zakupu dodatkowych licencji. 7. Zaimplementowanie w systemie operacyjnym środowiska wirtualizacyjnego musi umożliwiać dodawanie i usuwanie pamięci wirtualnej oraz wirtualnych kart sieciowych podczas pracy maszyny wirtualnej. 8. System operacyjny musi posiadać graficzny interfejs użytkownika. 9. System operacyjny musi być w pełni kompatybilny z usługą Active Directory w zakresie: a. zarządzania użytkownikami, b. zarządzania certyfikatami dla użytkowników wraz ze wsparciem możliwości logowania do domeny kartą mikroprocesorową, c. możliwości przydzielania praw dostępu do zasobów sieciowych, d. instalacji zdalnej oprogramowania z pakietów msi, e. definiowanie polityk bezpieczeństwa dla użytkowników, grup oraz stacji roboczych z systemami MS Windows: 7,8,8.1, 10,11. 10. System operacyjny musi wspierać pracę domenową wraz z automatyczną synchronizacją dla dodatkowych serwerów. 11. System operacyjny musi posiadać obsługę zdalnego pulpitu poprzez protokół RDP. 12. System operacyjny musi umożliwiać ustawianie relacji zaufania pomiędzy domenami. 13. Wszystkie narzędzia i usługi systemu operacyjnego powinny być rozwiązaniem jednego producenta. 14. System operacyjny musi posiadać obsługę pamięci USB jako monitora klastra

	15. System operacyjny musi pozwalać na stopniowe uaktualnienia systemu operacyjnego klastra 16. System operacyjny musi posiadać obsługę deduplikacji na potrzeby systemu plików ReFS. 17. System operacyjny musi posiadać obsługę optymalizacji transportu w tle pod kątem opóźnień. 18. System operacyjny musi posiadać wbudowaną zaporę internetową (firewall) dla ochrony połączeń internetowych; zapora musi być zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6; 19. System operacyjny musi posiadać możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny; 20. System operacyjny musi posiadać możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu; 21. System operacyjny musi posiadać obsługa PowerShell 5.1, 22. System operacyjny musi posiadać obsługa certyfikatów w Active Directory 23. Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte muszą być dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).

3. Miejsce dostawy, montażu, opieka powdrożeniowa

W ramach przedmiotu zamówienia Zamawiający wymaga:

1. Konfiguracja nowej macierzy oraz nowego serwera w serwerowni **Urzędu Miasta Mława przy ul. Stary Rynek 19, 06-500 Mława.**
2. Podłączenie do macierzy nowego serwera oraz obecnie funkcjonujących u Zamawiającego **Dell Power Edge R350; R730: R750;**
3. Instalacji systemu witalizacyjnego na nowym serwerze.
4. Instalacji w środowisku wirtualnym na serwerze systemu operacyjnego Windows Serwer 2025 lub równoważny wraz z konfiguracją primary domain, który ma być obsługiwany na nowym serwerze, a plik wirtualnego środowiska ma znajdować się na macierzy.
5. Instalacji CALI, konfiguracja podstawowych polityk domeny.
6. Przystosowanie posiadanego przez Zamawiającego serwera Dell Power Edge R350 do współpracy z nową macierzą, w tym reinstalacja/przystosowanie środowiska Vmware do obsługi wirtualnego systemu operacyjnego Windows Serwer 2025 secondary domain z macierzy.
7. W ramach instalacji nowej domeny Windows 2025 mają być wykonane operacje: przeniesienie obecnie funkcjonującej domeny w UM Mława (system Windows 2012) wraz z użytkownikami.
8. Przeniesienie musi być tak wykonane tak, aby nie było potrzeby reinstalacji/rekonfiguracji/zakładania nowych kont na komputerach użytkowników, użytkownicy mają zachować stare loginy, konta, pulpity, dane na komputerach.
9. 1 miesięczną dedykowaną opiekę powdrożeniową realizowaną zdalnie – wymagane jest, aby do opieki wyznaczony był dedykowany inżynier dostarczonego sprzętu i oprogramowania. Wsparcie powdrożeniowe musi być świadczone w dni robocze w godzinach 8:00 – 16:00.

2) Zamówienie dla Centrum Usług Społecznych w Mławie

1. Serwer z oprogramowaniem – 2 sztuki

Specyfikacje minimalnych wymagań:

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Obudowa Rack o wysokości max 1U z możliwością instalacji 8 dysków 2.5” • Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze.
Płyta główna	• Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Płyta powinna obsługiwać do min. 128GB, na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone dla pamięci
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych
Procesor	Jeden procesor Minimum 8 rdzeni fizycznych. Minimum 16 wątków logicznych (obsługa technologii wielowątkowości/Hyper-Threading). Bazowa częstotliwość taktowania procesora nie mniejsza niż 3,2 GHz. Maksymalna częstotliwość Turbo nie niższa niż 5,6 GHz. Pamięć podręczna trzeciego poziomu (L3) nie mniejsza niż 24 MB. Obsługa pamięci typu DDR5 Współczynnik TDP nie większy niż 95 W. Wynik nie mniejszy niż 95.1 punktów w teście SPECrate2017_int_base (w konfiguracji jednoprocesorowej), zgodnie z danymi opublikowanymi na stronie: https://www.spec.org. Wynik nie mniejszy niż 28 974 punktów w teście PassMark CPU Mark, zgodnie z danymi zawartymi na stronie: https://www.cpubenchmark.net.
Pamięć RAM	• 2x32GB pamięci RAM DDR5 UDIMM o częstotliwości pracy 5600MT/s.

Kontroler RAID	• Sprzętowy kontroler dyskowy, posiadający
	  ○ Min. 8GB nieulotnej pamięci cache,
	  ○ Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
	  ○ Wsparcie dla dysków samoszyfrujących

Dyski twarde	• Zainstalowane ○ 3x dysk SAS o pojemności min. 1.2TB, Hot-Plug. • Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
Sloty PCIe	• Dwa sloty PCIe
Interfejsy sieciowe/FC/SAS	• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT

Wbudowane porty	• min. 4 porty USB w tym min:
	  ○ 1 port USB 3.0 z tyłu obudowy,
	  ○ 1 port micro USB z przodu obudowy
	• 1 port VGA na tylnym panelu,
	• 1 port RS232

Karta graficzna	• Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
Zasilacze	• Redundantne, o mocy maks. 700W klasy Titanium
Elementy montażowe	• Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 V3 • Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).

Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:
	  ○ zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
	  ○ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
	  ○ szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;
	  ○ możliwość podmontowania zdalnych wirtualnych napędów;
	  ○ wirtualną konsolę z dostępem do myszy, klawiatury;
	  ○ wsparcie dla IPv6;
	  ○ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;
	  ○ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;
	  ○ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;
	  ○ integracja z Active Directory;
	  ○ możliwość obsługi przez dwóch administratorów jednocześnie;
	  ○ wsparcie dla dynamic DNS;
	  ○ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
	  ○ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
	  ○ możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
	oraz z możliwością rozszerzenia funkcjonalności o:
	  ○ Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej

	○ Przesyłanie danych telemetrycznych w czasie rzeczywistym ○ Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze ○ Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: ○ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych ○ integracja z Active Directory ○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta ○ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish ○ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram ○ Szczegółowy opis wykrytych systemów oraz ich komponentów ○ Możliwość eksportu raportu do CSV, HTML, XLS, PDF ○ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. ○ Grupowanie urządzeń w oparciu o kryteria użytkownika ○ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji ○ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach ○ Szybki podgląd stanu środowiska ○ Podsumowanie stanu dla każdego urządzenia ○ Szczegółowy status urządzenia/elementu/komponentu ○ Generowanie alertów przy zmianie stanu urządzenia. ○ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń ○ Integracja z service desk producenta dostarczonej platformy sprzętowej ○ Możliwość przejęcia zdalnego pulpitu ○ Możliwość podmontowania wirtualnego napędu ○ Kreator umożliwiający dostosowanie akcji dla wybranych alertów ○ Możliwość importu plików MIB ○ Przesyłanie alertów „as-is” do innych konsol firm trzecich ○ Możliwość definiowania ról administratorów ○ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów ○ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) ○ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta ○ Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów ○ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących

	alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. o Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. o Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile o Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. o Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. o Zdalne uruchamianie diagnostyki serwera. o Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. o Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: • Monitoring: o ilość podłączonych oraz rozłączonych systemów o stan podłączonych urządzeń o informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów o Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia o informacje o statusie gwarancji dla poszczególnych urządzeń o informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń o informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. o Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych o Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. o Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. o Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. o Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. o Monitoring parametrów serwerów z informacją o minimum: ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego

	▪ Zużyciu prądu ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. o Monitoring parametrów pamięci masowych z informacją o minimum: ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów o Monitoring parametrów przełączników sieciowych z informacją o minimum: ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ▪ Stanie komponentów: zasilacze, wentylatory ▪ Podłączonych hostach ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Aktualizacja firmware o możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty o Możliwość generowania raportów dla serwerów zawierających informację o: ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie

operacyjnym, protokole komunikacyjnym z systemem pamięci masowej
        - Średnim obciążeniu: procesorów, pamięci RAM, IO,
    - Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o:
        - Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji
    - Generowanie raportów do plików CSV i PDF
- Cyberbezpieczeństwo
    - Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia.
    - Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń.
    - Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.
    - Możliwość przypisania dedykowanych ról dla poszczególnych administratorów.
- Wspierane urządzenia
    - Urządzenie Producenta dostarczane w ramach postępowania
    - Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego)
- Wirtualny asystent
    - Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury;
- Możliwość rozszerzenia funkcjonalności
    - Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT.
- Inne
    - Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android
- Certyfikaty

Oferowana platforma musi być zaprojektowana zgodnie z zasadami zarządzania bezpieczeństwem informacji, co najmniej równoważnymi normie ISO/IEC 27001. Za równoważne uznaje się m.in. zgodność ze standardami:

- NIST SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations),
- CSA Cloud Controls Matrix (CCM),

lub innymi równoważnymi normami spełniającymi analogiczne wymagania dotyczące poufności, integralności i dostępności informacji.

Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku lub równoważnego certyfikatu środowiskowego potwierdzającego spełnienie porównywalnych wymagań dotyczących efektywności energetycznej, zawartości substancji niebezpiecznych, recyklingu i trwałości produktu - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.** • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Oprogramowanie serwerowe	**Oprogramowanie serwerowe – 2 sztuki dla każdego serwera, łącznie 4 szt.** Wymagane minimalne parametry System operacyjny Windows Server 2025 Standard (licencja na 16 rdzeni procesora, wersja OEM) lub równoważnego. Opis równoważności dla systemu Windows Server 2025 Standard: 1. System operacyjny musi być przeznaczony do zastosowań serwerowych w Środowiskach fizycznych lub o minimalnej wirtualizacji. 2. System operacyjny musi być najnowszą wersją rodziny systemów operacyjnych danego producenta. 3. Licencja na system operacyjny musi uwzględniać prawo do bezpłatnej instalacji udostępnianych przez producenta poprawek krytycznych i opcjonalnych do zakupionej wersji oprogramowania co najmniej przez 5 lat. 4. Licencja na system operacyjny musi umożliwiać uruchomienie kontrolera domeny. 5. Licencja na system operacyjny musi być bez ograniczeń czasowych. 6. Licencja na system operacyjny musi uprawniać do uruchamiania systemu operacyjnego w środowisku fizycznym i min. 2 środowiskach wirtualnych za pomocą wbudowanych mechanizmów wirtualizacji, bez konieczności zakupu dodatkowych licencji.

	7. Zaimplementowanie w systemie operacyjnym środowiska wirtualizacyjnego musi umożliwiać dodawanie i usuwanie pamięci wirtualnej oraz wirtualnych kart sieciowych podczas pracy maszyny wirtualnej. 8. System operacyjny musi posiadać graficzny interfejs użytkownika. 9. System operacyjny musi być w pełni kompatybilny z usługą Active Directory w zakresie: a. zarządzania użytkownikami, b. zarządzania certyfikatami dla użytkowników wraz ze wsparciem możliwości logowania do domeny kartą mikroprocesorową, c. możliwości przydzielania praw dostępu do zasobów sieciowych, d. instalacji zdalnej oprogramowania z pakietów msi, e. definiowanie polityk bezpieczeństwa dla użytkowników, grup oraz stacji roboczych z systemami MS Windows: 7,8,8.1, 10,11. 10. System operacyjny musi wspierać pracę domenową wraz z automatyczną synchronizacją dla dodatkowych serwerów. 11. System operacyjny musi posiadać obsługę zdalnego pulpitu poprzez protokół RDP. 12. System operacyjny musi umożliwiać ustawianie relacji zaufania pomiędzy domenami. 13. Wszystkie narzędzia i usługi systemu operacyjnego powinny być rozwiązaniem jednego producenta. 14. System operacyjny musi posiadać obsługę pamięci USB jako monitora klastra 15. System operacyjny musi pozwalać na stopniowe uaktualnienia systemu operacyjnego klastra 16. System operacyjny musi posiadać obsługę deduplikacji na potrzeby systemu plików ReFS. 17. System operacyjny musi posiadać obsługę optymalizacji transportu w tle pod kątem opóźnień. 18. System operacyjny musi posiadać wbudowaną zaporę internetową (firewall) dla ochrony połączeń internetowych; zapora musi być zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6; 19. System operacyjny musi posiadać możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny; 20. System operacyjny musi posiadać możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu; 21. System operacyjny musi posiadać obsługa PowerShelI 5.1, 22. System operacyjny musi posiadać obsługa certyfikatów w Active Directory 23. Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte muszą być dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).
Oprogramowanie serwerowe	**11** pakietów licencji dostępów klienckich (CAL) typu User. Licencje dostępowe typu Windows Server 2025 User CAL lub równoważnego: a. w łącznej liczbie **55 sztuk,** b. w postaci 11 pakietów po 5 licencji (5-pack), c. wersja: Windows Server CAL 2025 Polish 1pk DSP OEI 5 Clt User CAL,

	d. licencje wieczyste, przypisane do użytkownika (User CAL).

2. Miejsce dostawy, montażu i opieka powdrożeniowa

W ramach przedmiotu zamówienia Zamawiający wymaga:

1. Konfiguracji nowych serwerów w serwerowni **Centrum Usług Społecznych w Mławie ul. Lelewela 7, 06 – 500 Mława**.
2. Instalacji systemu operacyjnego oraz systemów virtualych Hyper-V lub równoważnych na nowych serwerach.
3. Instalacji na pierwszym serwerze wirtualnych systemów operacyjnych: jeden Windows Serwer 2025 lub równoważny wraz z **konfiguracją primary domain** oraz drugi wirtualny system operacyjny Windows Serwer 2025 lub równoważny.
4. Instalacji na drugim serwerze wirtualnych systemów operacyjnych: jeden Windows Serwer 2025 lub równoważny wraz z **konfiguracją secondary domain** oraz drugi wirtualny system operacyjny Windows Serwer 2025 lub równoważny.
5. Instalacji CALI, konfiguracji podstawowych polityk domeny.
6. 1 miesięcznej dedykowanej opieki powdrożeniowej realizowanej zdalnie – wymagane jest, aby do opieki wyznaczony był dedykowany inżynier dostarczonego sprzętu i oprogramowania. Wsparcie powdrożeniowe musi być świadczone w dni robocze w godzinach 8:00 – 16:00.

3) Warunki gwarancji i rękojmi oraz serwisu

1. Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres min. 36 miesięcy. **UWAGA:** wydłużenie okresu gwarancji stanowi kryterium II oceny oferty.
2. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.
3. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego (w przypadku krytycznych zgłoszeń) wyznaczonego Kierownika Eskalacji po stronie Producenta.
4. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.
5. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.
6. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.
7. **Dotyczy serwer z oprogramowaniem:** Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.

8. **Dotyczy macierz dyskowa:** Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym wstępnie na etapie diagnostyki) ma rozpocząć naprawę w siedzibie Zamawiającego najpóźniej w ciągu 4 godzin od zakończenia procesu diagnostycznego i podjąć starania przywrócenia sprzętu do stanu używalności od wysłania zasobów w ciągu 6 godzin (dla zgłoszeń o poziomie ważności 1) Naprawa ma się odbywać w siedzibie Zamawiającego, chyba, że Zamawiający dla danej naprawy zgodzi się na inną formę.
9. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.
10. Zamawiający, zgodnie z postanowieniami PPU (załącznik nr 2a do SWZ), wymaga od Wykonawcy, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
11. Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:
    a) Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie Zamawiającego.
    b) Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.
    c) Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.
    d) Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.
    e) Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.
12. Wymagane przedłożenie przed zawarciem umowy oświadczenia Producenta/Dystrybutora potwierdzającego, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta/Dystrybutora i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta/Dystrybutora.
13. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń (lub równoważny dokument potwierdzający zdolność do realizacji usług serwisowych zgodnie ze standardami producenta).

4) Wymagania ogólne dla dostarczanych rozwiązań

1. Dostarczone oprogramowanie musi być fabrycznie nowe, nieużywane, nieaktywowane wcześniej na innym urządzeniu, dostarczone w najnowszej stabilnej wersji pochodzącej z oficjalnego kanału dystrybucyjnego producenta oprogramowania nieobciążone prawami na rzecz osób trzecich. Dostarczone oprogramowanie i wszelkie jego nośniki (o ile występują) musi być wolne od wad fizycznych i prawnych.
2. Dostarczony SPRZĘT, musi być fabrycznie nowy, nieużywany, nieregenerowany, kompletny, wyprodukowany nie wcześniej niż w styczniu 2024 r., dostarczony w opakowaniu oryginalnym (opakowanie musi być nienaruszone i posiadać zabezpieczenie zastosowane przez producenta/dystrybutora). Sprzęt musi być wolny od jakichkolwiek wad fizycznych i prawnych, sprawny technicznie oraz musi pochodzić z autoryzowanego kanału dystrybucyjnego. Nie dopuszcza się zastosowania urządzeń tzw. „refurbished".
3. Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów w okresie zapisanym w specyfikacjach sprzętu.
4. Całość dostarczonego oprogramowania musi być ze sobą kompatybilna.
5. Zamawiający uzyska dostęp do stron internetowych producentów rozwiązań, umożliwiający:
   a) bezpłatne pobieranie najnowszego oprogramowania aktualizującego system do najnowszej wersji przez okres trwania licencji,
   b) dostęp do dokumentacji sprzętu i oprogramowania,
   c) dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej,
   d) dostęp do pomocy technicznej producenta.