Ministerstwo Rozwoju i Technologii **Warszawa, 25.09.2025 r.**

ul. Plac Trzech Krzyży 3/5

00-507 Warszawa

ZAPYTANIE O WYCENĘ DO OSZACOWANIA WARTOŚCI ZAMÓWIENIA

Ministerstwo planuje uruchomić postępowanie przetargowe o udzielenie zamówienia publicznego na rozbudowę infrastruktury serwerowej.

Uprzejmie prosimy o wycenę, poniżej opisanych minimalnych wymagań stanowiących przedmiot planowanego do wszczęcia postępowania przetargowego.

Zamówienie zostanie podzielone na trzy części:

1. Część I, tj. dostawa 6 serwerów wraz ze wsparciem na 36 miesięcy oraz licencjami oprogramowania wirtualizacji
2. Część II, tj. dostawa licencji systemów operacyjnych
3. Część III, tj. dostawa macierzy all-flash oraz przełączników fibre channel wraz ze wsparciem na 60 miesięcy

Zamawiający zamierza podzielić zamówienie na części. Tym samym Zamawiający dopuszcza składanie ofert częściowych, tj. Wykonawca może złożyć ofertę na jedną, dwie lub trzy części zamówienia.

Część I

Zakres zamówienia

Lp.	Produkt	Liczba sztuk
1	Serwer wraz ze wsparciem na 36 miesięcy	6
2	Licencja oprogramowania wirtualizacji dla dostarczanych klastrów ze wsparciem na 36 miesięcy	384 core fizyczne
3	Usługa wdrożenia oraz instruktażu	1

Część II

Zakres zamówienia

Lp.	Numer katalogowy	Produkt	Rodzaj licencjonowania	Liczba produktów
1	9EA-00271	Win Server DC Core ALng LSA 16L z Software Assurance ważnym od dostarczenia do 30.06.2028 r.	Nieograniczona w czasie	6
2	9EA-00039	Win Server DC Core ALng LSA 2L z Software Assurance ważnym od dostarczenia do 30.06.2028 r.	Nieograniczona w czasie	144

Część III

Zakres zamówienia

Lp.	Produkt	Liczba produktów
1	Dostawa macierzy all-flash wraz z wsparciem na 60 miesięcy	1
2	Dostawa nowych przełączników fibre channel wraz z wsparciem na 60 miesięcy	2
3	Rozbudowa licencji o 8 portów w posiadanych przez Zamawiającego przełącznikach fibre channel	2
4	Usługa wdrożenia oraz instruktażu	1

I. PRZEDMIOT ZAMÓWIENIA

Przedmiotem Zamówienia, jest rozbudowa infrastruktury serwerowej.

Zamówienie obejmuje:

Część I, tj. dostawę 6 serwerów, które muszą tworzyć 2 klastry składające się z 3 serwerów wraz ze wsparciem na 36 miesięcy, w tym:

1. Dostawę 3 serwerów dla klastra wirtualizacji, tj. elementów infrastruktury przeznaczonych do uruchomienia klastra wraz ze wsparciem producenta na okres 36 miesięcy do podstawowego ośrodka Zamawiającego.
2. Dostawę 3 serwerów klastra wirtualizacji, tj. elementów infrastruktury przeznaczonych do uruchomienia klastra wraz ze wsparciem producenta na okres 36 miesięcy do zapasowego ośrodka Zamawiającego.
3. Dostawę licencji oprogramowania wirtualizacji dla dostarczanych klastrów ze wsparciem na 36 miesięcy.
4. Wdrożenie dostarczonych elementów, w tym:
   a) instalację dostarczonych urządzeń i subskrypcji oprogramowania,
   b) konfigurację, uruchomienie i testowanie, w tym dodatkowych elementów,
   c) wykonanie dokumentacji technicznej i eksploatacyjnej,
   d) przeprowadzenie instruktażu dla administratorów Systemu.

Część II, tj. dostawę licencji systemów operacyjnych, w tym dostawa licencji Microsoft Windows Datacenter wraz z Software Assurance

Część III, tj. dostawę macierzy all-flash oraz przełączników fibre channel wraz ze wsparciem na 60 miesięcy w tym:

1. dostawa macierzy all-flash tj. elementów infrastruktury przeznaczonych do uruchomienia macierzy wraz ze wsparciem producenta na okres 60 miesięcy do podstawowego ośrodka Zamawiającego;
2. dostawa przełączników fibre channel tj. elementów infrastruktury przeznaczonych do uruchomienia przełączników wraz ze wsparciem producenta na okres 60 miesięcy do podstawowego ośrodka Zamawiającego;
3. dostawa rozbudowy licencji o 8 portów do posiadanych przez Zamawiającego przełączników fibre channel zlokalizowanych w zapasowym ośrodku Zamawiającego;
4. usługa wdrożenia i instruktażu.

II. TERMIN REALIZACJI ZAMÓWIENIA

Przedmiot zamówienia zostanie zrealizowany w terminie maksymalnie **do 40 dni** od daty podpisania przez strony umowy **(termin realizacji do uzupełnienia przez Wykonawcę w Formularzu Ofertowym).**

Realizacja przedmiotu zamówienia obejmować będzie dostawę zakup klastra serwerów baz danych wraz z niezbędnymi licencjami technologicznymi dla Ministerstwa Rozwoju i Technologii do centrum przetwarzania na terenie Polski wskazanego przez Zamawiającego.

III. MINIMALNE WYMAGANIA DOTYCZĄCE REALIZACJI PRZEDMIOTU ZAMÓWIENIA

1. Zaoferowane urządzenia oraz oprogramowanie nie może być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.
2. Wszystkie elementy dostarczone z urządzeniami, będą pochodziły od jednego producenta. Stosowane elementy muszą być wspierane przez producenta urządzeń i być objęte możliwością analizy potencjalnych błędów w trakcie potencjalnych zgłoszeń serwisowych. Muszą pochodzić z autoryzowanego kanału sprzedaży producentów Urządzeń na rynek polski lub Unii Europejskiej
3. Zaoferowane urządzenia muszą być fabrycznie nowe przeznaczone do sprzedaży na rynku europejskim (zgodnie z ustawą z dnia 30.08.2002 r. o systemie oceny zgodności (Dz.U. z 2004 r., nr 204, poz. 2087 j.t. z późn. zm.) i z wydanymi na jej podstawie rozporządzeniami), wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia oraz objęte wymaganą przez Zamawiającego gwarancją w Polsce. Zamawiający nie dopuszcza produktów „odnawianych" (ang. Refurbished). Zaoferowane urządzenia, oprogramowanie sterujące połączeniami oraz aplikacje zarządzające muszą pochodzić od tego samego producenta. Zamawiający wymaga, aby dostarczony System pochodził z oficjalnego kanału dystrybucyjnego danego producenta, a serwis gwarancyjny był autoryzowany przez producenta urządzeń i oprogramowania oraz świadczony przez producenta lub autoryzowanych partnerów w centrach serwisowych na terenie Unii Europejskiej.
4. Zamawiający wymaga, aby zaoferowane urządzenia były dostępne i serwisowane przez Producenta oraz nie będą przez niego przewidziane do wycofania ze sprzedaży i wsparcia

(ogłoszone tzw. dokumenty End-of-Sale lub End-of-Life lub równoważne) – na dzień składania oferty.

IV. MINIMALNE WYMAGANIA TECHNICZNE I FUNKCJONALNE KLASTRÓW WIRTUALIZACJI

1. Każdy klaster wirtualizacji musi składać się z minimum 3 serwerów fizycznych.
2. Każdy z serwerów musi być wyposażony w 2 procesory x86 wyposażony w 32 rdzenie fizycznych i z bazowym taktowaniem minimum 3.1 Ghz i osiągające w testach SPECrate2017_int_base wynik nie gorszy niż 790 punktów, dla testu oferowanego modelu serwera z 2 procesorami.
3. Obudowa Rack o wysokości max. 2U z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych z organizerem do kabli.
4. Płyta główna z możliwością zainstalowania dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
5. Chipset dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
6. RAM Min. 2TB DDR5 RDIMM 6400MT/s w modułach pamięci o pojemności min. 64GB każdy. Na płycie głównej powinno znajdować się minimum 32 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 8TB pamięci RAM.
7. Zabezpieczenia pamięci RAM: Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection
8. Gniazda PCIe - minimum dwa sloty PCIe x16 generacji 5 i dwa sloty OCP.
9. Interfejsy sieciowe/FC/SAS: Dwa interfejsy sieciowe 25Gb Ethernet ze złączami SFP28 i cztery interfejsy sieciowe 1Gb Ethernet ze złączami Base-T nie zajmujące slotów PCIe.
   Dodatkowo zainstalowane:
   - jedna karta dwuportowa 25Gb Ethernet ze złączami SFP28.
   - jedna karta dwuportowa FC 32Gb/s
10. Każdy serwer powinien zostać dostarczony wraz z
    a. 2 wkładkami SFP+, wielomodowymi, krótkodystansowymi, ze złączem LC o prędkości 32 Gbit każda.
    b. 4 aktywnych kabli optycznych AOC SFP28 25Gbps o długości 5 metrów. Kable muszą posiadać certyfikację producenta Cisco posiadanych przez Zamawiającego.
11. Dyski twarde:
    Zainstalowany 1 x 1.6TB NVMe E3s, DWPD min. 3.
    Zainstalowane dwa dyski hot-swap M.2 NVMe o pojemności min. 480GB z możliwością konfiguracji RAID 1.
12. Kontroler RAID: Sprzętowy kontroler dyskowy z pojemnością cache 8GB, możliwe konfiguracje poziomów RAID: 0,1,5,6,10,50,60, non-RAID (JBOD). Obsługa najnowszego standardu transmisji danych w technologii PCIe generacji 5 , umożliwiającego pełne wykorzystanie wydajności nośników NVMe.
13. Wbudowane porty min. port USB 2.0 oraz dwa porty USB 3.1, port VGA,
14. Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900
15. Wentylatory Redundantne Hot-Plug
16. Zasilacze Min. dwa zasilacze Hot-Plug min. 1500W Titanium.
17. Każdy serwer musi zostać dostarczony przewodami zasilającymi kompatybilnymi z infrastrukturą Zamawiającego. Zamawiający w udostępnionej przestrzeni szaf rack posiada złącza C13 i C19.
18. Bezpieczeństwo:
    - Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła
    - Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą TPM 2.0 Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem. Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania.
19. Karta Zarządzania:
    - Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:
    - zdalny dostęp do graficznego interfejsu Web karty zarządzającej
    - 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 SNMP; IPMI2.0, VLAN tagging, SSH

- możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz.
- możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer
- integracja z Active Directory
- możliwość obsługi przez ośmiu administratorów jednocześnie
- Wsparcie dla automatycznej rejestracji DNS
- wsparcie dla LLDP
- wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej
- możliwość podłączenia lokalnego za pomocą interfejsu USB-C na froncie serwera, który pozwala na bezpośredni dostęp interfejsu karty zarządzającej (zarówno UI w przeglądarce, jak i konsolę RACADM czy API Redfish) bez potrzeby połączenia sieciowego
- Monitorowanie zużycia dysków SSD
- możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi,
- Automatyczne zgłaszanie alertów do centrum serwisowego producenta
- Automatyczne update firmware dla wszystkich komponentów serwera
- Możliwość przywrócenia poprzednich wersji firmware
- Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON
- Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych
- Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram.
- Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera

20. Oprogramowanie do zarządzania.

    Zainstalowane oprogramowanie producenta serwera do zarządzania, spełniające 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.

- 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.

21. Normy Środowiskowe:

    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 rozporządzenia nr 1272/2008WE. 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 - Wykonawca złoży dokument potwierdzający spełnianie wymogu. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta serwera

22. Certyfikaty:
    - Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001.
    - Serwer musi posiadać deklaracja CE. Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 lub oświadczenie producenta o stosowaniu w fabrykach polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej.
    - Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2022 x64, Microsoft Windows 2025.

V. MINIMALNE WYMAGANIA TECHNICZNE I FUNKCJONALNE OPROGRAMOWANIA WIRTUALIZACJI

1. Wszystkie licencje zaoferowanego oprogramowania do wirtualizacji muszą być licencjami subskrypcyjnymi, tj. licencja na określony czas w formularzu technicznym wraz ze wsparciem technicznym do tych licencji świadczonym przez producenta zaoferowanego oprogramowania. Ilość licencji musi uwzględniać parametry serwerów do wirtualizacji (6 serwerów dwuprocesorowych z procesorami trzydziesto-dwu rdzeniowymi).
2. Wszystkie wymagane poniżej komponenty/moduły muszą pochodzić od jednego producenta oprogramowania.
3. Licencje zaoferowanego oprogramowania muszą być zaoferowane w formie „per core” fizyczny procesora fizycznego.
4. Zaoferowane oprogramowanie musi być instalowane bezpośrednio na sprzęcie fizycznym i nie może być ono częścią innego systemu operacyjnego.
5. Zaoferowane oprogramowanie musi być instalowane bezpośrednio na sprzęcie fizycznym i nie może być ono częścią innego systemu operacyjnego.
6. W zaoferowanym oprogramowaniu warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 700MB pamięci operacyjnej RAM serwera fizycznego
7. Zaoferowane oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi potrafić obsłużyć i wykorzystać procesory fizyczne tego serwera wyposażone w 768 logicznych wątków, 24TB pamięci fizycznej RAM tego serwera oraz 16 procesorów fizycznych tego serwera.
8. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z ilością od 1 do 768 procesorów wirtualnych
9. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 24 TB pamięci operacyjnej RAM.
10. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia od 1 do 10 wirtualnych kart sieciowych dla każdej z nich. Dodatkowo, oprogramowanie musi posiadać możliwość utworzenia maszyny wirtualnej bez przydzielonej wirtualnej karty sieciowej.

11. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe, 3 porty równoległe i 20 urządzeń USB.
12. Zaoferowane oprogramowanie musi wspierać minimum następujące systemy operacyjne: Windows Server 2012/2016/2019/2022, Windows 8/10/11, RHEL 6/7/8/9, SLES 12/15, Debian 10/11, CentOS 7/8, Ubuntu 16/18/20/22, Photon OS 2/3/4, Oracle Linux 6/7/8/9, FreeBSD 12/13.
13. W celu osiągnięcia maksymalnego współczynnika konsolidacji, zaoferowane oprogramowanie musi umożliwiać przydzielenie łącznie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera, na którym maszyny te są posadowione.
14. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie dostępne na zasobach dyskowych
15. Zaoferowane oprogramowanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji bez ingerencji w systemy operacyjne maszyn wirtualnych (bezagentowość).
16. Zaoferowane oprogramowanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta „root”
17. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość powielania maszyn wirtualnych wraz z ich pełną konfiguracją i danymi
18. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością konieczności zachowania stanu pamięci pracującej maszyny wirtualnej.
19. Konsola zarządzająca zaoferowanego oprogramowania musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, minimalnie z: Microsoft Active Directory i Open LDAP oraz umożliwiać federacyjne zarządzanie tożsamością w oparciu o Microsoft Active Directory Federation Services (ADFS).
20. Zaoferowane oprogramowanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej
21. Zaoferowane oprogramowanie musi posiadać funkcjonalność tworzenia wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta (hypervisora wirtualizacyjnego) i pozwalającego połączyć tym przełącznikiem maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji aż do 4096 portów
22. Pojedynczy wirtualny przełącznik w zaoferowanym oprogramowaniu, w celu zapewnienia bezpieczeństwa połączenia ethernetowego w razie awarii fizycznej karty sieciowej, musi posiadać możliwość przyłączania do niego minimum dwóch fizycznych kart sieciowych
23. Wirtualne przełączniki w zaoferowane oprogramowaniu muszą posiadać funkcjonalność obsługi wirtualnych sieci lokalnych (VLAN)
24. Zaoferowane oprogramowanie musi umożliwiać wykorzystanie technologii przepustowości sieci komputerowych do 200GbE poprzez agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi
25. Zaoferowane oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek
26. Zaoferowane oprogramowanie musi zapewnić możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych
27. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi zapewniać możliwość replikacji maszyn wirtualnych z dowolnej pamięci masowej w tym z dysków wewnętrznych serwerów fizycznych na dowolną pamięć masową w tym samym lub oddalonym ośrodku przetwarzania. Replikacja musi gwarantować współczynnik RPO (ang. Recovery Point Objective) na poziomie minimum 5 minut
28. Zaoferowane oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek
29. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi mieć możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi bez przerywania pracy usług na przenoszonych maszynach wirtualnych. Wymaga się wsparcia natywnego szyfrowania ruchu sieciowego dla maszyn wirtualnych podczas ich przenoszenia między serwerami fizycznymi
30. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter oraz w środowisku z więcej niż pojedynczym wirtualizatorem, musi umożliwiać automatyczne, ponowne uruchomienie maszyn wirtualnych w przypadku awarii jednego z wirtualizatorów na kolejnym, działającym w tym samym klastrze wirtualizatorze (funkcjonalność HA) (ang. High Availability)
31. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter w środowisku z minimalnie dwoma wirtualizatorami oraz w przypadku potrzeby wgrania aktualizacji do warstwy wirtualizacji, musi posiadać możliwość w przypadku wywołania startu

aktualizacji, automatycznego przeniesienia bezprzerwowego działających maszyn wirtualnych do innego wirtualizatora nie objętego aktualizacją, przed rozpoczęciem samej aktualizacji
32. Zaoferowane oprogramowanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami z zainstalowanym wirtualizatorem oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci
33. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, w środowisku z minimum dwoma wirtualizatorami, musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (o maksymalnie dwóch procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii wirtualizatora, bez utraty danych i dostępności danych na maszynach wirtualnych objętych ochroną
34. Zaoferowane oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości 62 TB
35. Zaoferowane oprogramowanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej
36. Producent zaoferowanego oprogramowania do wirtualizacji musi wspierać rozwiązania do automatyzacji procesów oraz wirtualizacji sieci (SDN, ang. Software Defined Network).
37. Zaoferowane oprogramowanie musi wspierać mechanizmy zaawansowanego uwierzytelniania do systemu operacyjnego wirtualnej maszyny za pomocą technologii Smart Card Reader
38. Zaoferowane oprogramowanie musi wspierać TPM 2.0. Minimalne wymaganie Zamawiającego dla TPM oznacza, że TPM zapewnia mechanizm gwarantujący, że serwer fizyczny, na którym zainstalowane jest zaoferowane oprogramowanie, uruchomił się z włączoną opcją Secure Boot. Po potwierdzeniu, że Secure Boot jest włączone, system gwarantuje, poprzez weryfikację podpisu cyfrowego, że hypervisor uruchomił się w niezmienionej formie
39. Wirtualizator w zaoferowanym oprogramowaniu musi mieć możliwość włączenia funkcji “Microsoft virtualization-based security”, tzw. Microsoft VBS dla systemów operacyjnych maszyn wirtualnych opartych o system operacyjny Microsoft Windows 10, Microsoft Windows Server 2016 oraz Microsoft Windows Server 2019
40. Zaoferowane oprogramowanie musi posiadać certyfikację FIPS-140-2 min. dla modułu jądra wirtualizatora odpowiedzialnego za szyfrowanie danych
41. Zaoferowane oprogramowanie musi posiadać funkcjonalność wirtualnego TPM 2.0 dla maszyn wirtualnych z zainstalowanym Microsoft Windows 10 oraz Microsoft Windows 2016. Zamawiający wymaga, aby z punktu widzenia maszyny wirtualnej z systemem operacyjnym Microsoft Windows 10 lub Microsoft Windows 2016 wirtualny TPM widziany był jako standardowy TPM, gdzie można przechowywać bezpiecznie wrażliwe dane np. certyfikaty. Zawartość wirtualnego TPM musi być przechowywana w pliku przynależnym do maszyny wirtualnej oraz musi być szyfrowana.
42. Zaoferowane oprogramowanie musi posiadać funkcjonalność szybkiego uruchamiania wirtualizatora po przeprowadzonym procesie jego aktualizacji. Zamawiający wymaga, aby w procesie aktualizacji wirtualizatora, jeśli wymagany jest jego restart, funkcjonalność szybkiego uruchamiania powodowała eliminację czasochłonnej fazy inicjalizacji serwera fizycznego
43. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra, musi posiadać możliwość aktualizacji i kontroli wersji oprogramowania do wirtualizacji w ramach klastra serwerów z poziomu centralnej konsoli zarządzającej. Dodatkowo centralna konsola zarządzająca musi posiadać funkcjonalność aktualizacji firmware komponentów serwera fizycznego (dyski, kontrolery, karty sieciowe) z poziomu konsoli zarządzającej wirtualizatora. Konsola zarządzająca musi mieć możliwość automatycznej weryfikacji, czy zainstalowane komponenty serwera posiadają rekomendowaną wersję sterowników i firmware, eliminując ryzyko pracy na nieaktualnych wersjach. Taka funkcjonalność powinna być dostępna dla minimum dwóch producentów serwerów obecnych na rynku
44. Zaoferowane oprogramowanie musi posiadać wsparcie dla natywnych dysków 4K
45. Zaoferowane oprogramowanie musi wspierać protokół precyzyjnej synchronizacji czasu PTP (ang. Precision Time Protocol)
46. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra, musi posiadać mechanizm, który ogranicza dostęp do indywidualnego zarządzania warstwą wirtualizacji na serwerach fizycznych w ramach klastra serwerów w celu utwardzenia/hardening (maksymalnego zwiększenia bezpieczeństwa dostępu) systemu wirtualizacji.
47. Zaoferowane oprogramowanie musi mieć funkcjonalność migracji w trybie rzeczywistym dysków działających maszyn wirtualnych z jednego podsystemu dyskowego do innego bez konieczności przerywania pracy maszyny wirtualnej, której dysk jest migrowany
48. Zaoferowane oprogramowanie obejmuje walidację FIPS, a także zaktualizowane przewodniki audytów.
49. Zaoferowane oprogramowanie musi mieć możliwość utworzenia, poprzez API, maszyny wirtualnej jako tzw. Instant Clone poprzez klonowanie działającej maszyny wirtualnej w wyniku którego powstanie nowa działająca maszyna wirtualna identyczna z klonowaną. Nowa maszyna wirtualna musi powstawać w pamięci operacyjnej wirtualizatora

50. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra, musi mieć możliwość monitorowania i wyświetlania za pomocą grafu w konsoli bieżącego poboru energii elektrycznej dla hosta wirtualizacyjnego oraz dla maszyn wirtualnych na nim posadowionych
51. Ilość instancji zaoferowanego oprogramowania do zarządzania klastrem wirtualizacyjnym musi być równa liczbie fizycznych core zaoferowanych w oprogramowaniu do wirtulizacji mocy obliczeniowej
52. Zaoferowane oprogramowanie musi posiadać konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. min: zasobów dyskowych oraz zasobów sieci komputerowej. Konsola graficzna powinna działać jako zainstalowana aplikacja na maszynie wirtualnej. Dodatkowo wymaga się, aby maszyna z aplikacją była wstępnie skonfigurowana i dostępna jako tzw. virtual appliance. Instalacja w/w virtaul appliance nie może wiązać się z potrzebą dostawy dodatkowego oprogramowania takiego jak np. system operacyjny lub baza danych.
53. Zaoferowane oprogramowanie musi posiadać wbudowany serwer ściany ogniowej (ang. firewall) dający możliwość konfiguracji blokady lub akceptacji ruchu pomiędzy konsolą zarządzającą a serwerami oraz serwerami wirtualnymi na nich posadowionymi, przy założeniu blokowania całego ruchu a nie poszczególnych portów
54. Zaoferowane oprogramowanie musi mieć możliwość konfiguracji uwierzytelniania użytkowników logujących się do niego w oparciu o minimum: domenę Microsoft Active Directory, Microsoft Active Directory over LDAP oraz Open LDAP.
55. Zaoferowane oprogramowanie musi posiadać konsole graficzną, która musi być dostępna poprzez dedykowanego klienta (za pomocą przeglądarek minimum Mozilla Firefox oraz Chrome) lub poprzez konsolę graficzną, która zbudowana jest z wykorzystaniem języka HTML5
56. Zaoferowane oprogramowanie musi posiadać funkcjonalność zcentralizowanego zarządzania hostami VMware vSphere.
57. Zaoferowane oprogramowanie musi posiadać natywne mechanizmy do wykonywania kopii zapasowej swojej konfiguracji. Dodatkowo wymaga się możliwości ustawienia harmonogramu wykonywania kopii zapasowej. Wymaga się aby kopie zapasowe wspierały protokoły: FTPS, HTTPS, SCP, FTP oraz http.
58. Zaoferowane oprogramowanie, poprzez rozszerzenie o dodatkową licencję oferowaną przez tego samego producenta musi posiadać wbudowaną funkcjonalność zarządzania wirtualną przestrzenią dyskową SDS (ang. Software Defined Storage).
59. Zaoferowane oprogramowanie musi posiadać interfejs graficzny do prowadzenia prac administracyjnych w zakresie swojej konfiguracji oraz monitoringu (możliwość monitorowania obciążenia min. vCPU, vRAM, vHDD, sieci, bazy danych). Interfejs graficzny powinien być wykonany w standardzie HTML5
60. Zaoferowane oprogramowanie zawiera możliwość automatyzacji instalacji wielu konsoli zarządzania poprzez użycie schematów konfiguracji.
61. Zaoferowane oprogramowanie umożliwia aktualizowanie wielu wirtualizatorów równocześnie.
62. Rozwiązanie musi pozwalać na wykorzystanie łącz o szybkości do 100 GbE do bezawaryjnego przenoszenia maszyn wirtualnych między wirtualizatorami.
63. Rozwiązanie musi zapewniać natywne mechanizmy wysokiej dostępności HA (ang. High Availability) w niezawodnej architekturze Active-Passive-Witness dla wszystkich składowych komponentów centralnej konsoli graficznej zarządzającej platformą wirtualną.
64. Zaoferowane oprogramowanie zapewnia podstawowe funkcje serwera zarządzania kluczami (KMS), które upraszcza włączenie szyfrowania i zaawansowanych funkcji bezpieczeństwa.
65. Zaoferowane oprogramowanie, w przypadku zarządzania serwerami opartymi o VMware vSphere, musi prezentować poziom zbalansowania mocy obliczeniowej w klastrze opartym o w/w wirtualizatory.
66. Dostęp przez przeglądarkę do konsoli graficznej w zaoferowanym oprogramowaniu musi być skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska.

VI. MINIMALNE WYMAGANIA TECHNICZNE I FUNKCJONALNE DLA OPROGRAMOWANIA WINDOWS SERVER DATACENTER

1. Dla każdego z serwerów wirtualizacji należy dostarczyć wieczystą licencję typu Gov dla systemu operacyjnego Microsoft Windows Server Datacenter 2022 z możliwością przeniesienia licencji na inny serwer tego samego producenta.
2. Licencje na serwerowy system operacyjny muszą uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i nielimitowanej liczbie wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
3. Dodatkowo musi pozwalać na uruchamianie wirtualnych środowisk serwerowego systemu operacyjnego w usłudze hostowanej platformy producenta serwerowego systemu operacyjnego.
4. Oferowane Produkty muszą być produktami standardowymi – powszechnie dostępnymi na rynku (typu Commercial off-the-shelf - COTS).
5. Zamawiający nie dopuszcza zaoferowania licencji w modelu CSP.

6. Licencja musi być z Software Assurance ważnym do 30.06.2028 r. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy:
   a. Możliwość wykorzystania 512 logicznych procesorów oraz co najmniej 24 TB pamięci RAM w środowisku fizycznym.
   b. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
   c. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
   d. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
   e. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
   f. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
   g. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
   h. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
   i. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
      - pozwalają na zmianę rozmiaru w czasie pracy systemu,
      - umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym)
      - prosty wgląd w poprzednie wersje plików i folderów,
      - umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
      - umożliwiają zdefiniowanie list kontroli dostępu (ACL).
   j. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
   k. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez
   l. NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
   m. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET
   n. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
   o. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
   p. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
      - Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
      - Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
   q. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
   r. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
   s. Mechanizmy logowania w oparciu o:
      - Login i hasło,
      - Karty z certyfikatami (smartcard),
      - Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
   t. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
   u. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
   v. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
   w. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
   x. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
   y. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
   z. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
      - Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,

- Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
  1. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
  2. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
  3. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
     - Zdalna dystrybucja oprogramowania na stacje robocze,
     - Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,
     - Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
       1. Dystrybucję certyfikatów poprzez http,
       2. Konsolidację CA dla wielu lasów domeny,
       3. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
       4. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
     - Szyfrowanie plików i folderów.
     - Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
     - Możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów.
     - Serwis udostępniania stron WWW.
     - Wsparcie dla protokołu IP w wersjach 4 oraz 6 (IPv4; IPv6).
     - Wsparcie dla algorytmów Suite B (RFC 4869).
     - Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.
     - Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.
     - Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
       1. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
       2. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
       3. Obsługi 4-KB sektorów dysków
       4. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
       5. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
       6. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

aa. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.

bb. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).

cc. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.

dd. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji poprzez skrypty.

ee. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

ff. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

VII. MINIMALNE WYMAGANIA TECHNICZNE I FUNKCJONALNE MACIERZY ALL-FLASH

1. Macierz musi być przystosowana do montażu w szafie rack 19”.
2. Macierz musi być wyposażona w minimum 2 kontrolery.

3. Do urządzenia należy dołączyć kable połączeniowe zgodne z ilością portów i rodzajem zainstalowanych modułów.
4. Oferowane rozwiązanie musi zawierać się w obudowie maksymalnej wysokości 4U
5. Macierz musi być wyposażona w minimum 24 dysków SSD NVMe o pojemności nie mniejszej niż 15.36 TB zapewniającej minimum 248 TB przestrzeni użytkowej dla hostów bez stosowania mechanizmów deduplikacji i kompresji, i przy zapewnieniu odporności na awarię co najmniej 2 dowolnych dysków.
6. Nie dopuszcza się stosowania protokołu innego niż NVMe do obsługi dysków w macierzy.
7. Nie dopuszcza się stosowania dysków QLC. Wymagane są dyski MLC lub TLC.
8. Macierz musi mieć możliwość obsługi co najmniej 1PB pojemności surowej (raw) na dyskach SSD NVMe. Nie dopuszcza się stosowania dysków SSD SAS ani żadnych innych nośników poza SSD NVMe. Nie dopuszcza się wirtualizacji zewnętrznych pamięci masowych.
9. Macierz musi umożliwić rozbudowę do minimum 72 dysków SSD NVMe.
10. Macierz w dostarczonej konfiguracji (z włączoną deduplikacją i kompresją) musi umożliwiać osiągnięcie wydajności minimum 180 tysięcy IOPS z przestrzeni dyskowej (przy założeniach: dla bloku danych o wielkości 8k odczyt 70%, zapis 30% oraz wszystkie operacje losowe, 0% trafień w cache)
11. W zaproponowanej konfiguracji macierzy należy także zabezpieczyć przestrzeń hot/spare według zaleceń producenta macierzy. Niedopuszczalne jest zastosowanie dedykowanych dysków jako dyski hot-spare.
12. Do oferty należy dołączyć wydruk z narzędzia producenta oferowanej macierzy konfiguratora / estymatora – potwierdzony przez producenta, potwierdzający spełnienie powyższych wymagań (zawierający zarówno proponowaną konfigurację sprzętową z dokładnym wskazaniem part number'ów elementów jak i ich ilości, w tym typów i okresów wsparcia licencji i gwarancji) jak i wynikające z niej parametry pojemnościowe i wydajnościowe)
13. Macierz musi posiadać mechanizm RAID zabezpieczający przed utratą spójności danych w przypadku jednoczesnej awarii dwóch dowolnych dysków. Mechanizm realizowany sprzętowo za pomocą dedykowanego układu z wykorzystaniem puli wszystkich dysków twardych (tzw. wide-striping). lub równoważny.
14. Przez mechanizm równoważny należy rozumieć mechanizm programowy z wykorzystaniem puli wszystkich dysków twardych, zapewniający identyczny poziom zabezpieczenia danych i wydajności systemu a także wymaganej przestrzeni dyskowej.
15. Rozłożenie dysków w macierzy musi zapewniać redundancję pozwalającą na nieprzerwaną pracę i dostęp do wszystkich danych w sytuacji awarii pojedynczego komponentu sprzętowego typu: dysk, port, kontroler, zasilacz, kabel. Macierz musi umożliwiać definiowanie dysków „spare" lub odpowiadającej im przestrzeni dyskowej „spare". Wymagane zabezpieczenie minimum RAID-6.
16. Macierz musi być odporna na awarię pamięci cache, w szczególności cache przeznaczony do zapisu (ang. write cache) i zapewniać w razie utraty zasilania zabezpieczenie danych niezapisanych na dyski przez nieograniczony czas.
17. Macierz All-NVMe wyposażona w minimum 2 kontrolery macierzowe obsługujące protokoły blokowe i pracujące w trybie ALUA (Asymmetric Logical Unit Access).
18. Oba kontrolery muszą jednocześnie aktywnie obsługiwać wolumeny. Oprogramowanie macierzy musi rozkładać obsługę wolumenów pomiędzy kontrolery i dążyć do ich równomiernego obciążenia.
19. Kontrolery te muszą działać w sposób redundantny – tj. przy uszkodzeniu dowolnego kontrolera, macierz musi nadal działać i utrzymywać dostęp do odczytu i zapisu danych. Praca w trybie active/active w taki sposób, aby oba kontrolery były aktywne i w tym samym czasie udostępniały urządzenia LUN oraz zasoby plikowe. Oba kontrolery muszą brać czynny udział w obsłudze wszystkich operacji (snapshot, clone, replikacja). Nie dopuszcza się rozwiązania, w którym jeden z kontrolerów działa jedynie jako urządzenie przekazujące ruch do hostów.
20. Każdy z kontrolerów musi być wyposażony w wielordzeniowe procesory x86 (każdy w minimum 16 fizycznych rdzeni).
21. Z uwagi na kompatybilność z systemami operacyjnymi oraz aplikacjami występującymi w środowisku Zamawiającego, a listą rozkazów obsługiwanych przez procesory zainstalowane w oferowanym rozwiązaniu, Zamawiający zaakceptuje jedynie rozwiązania wyposażone w procesory firm Intel lub AMD. Zastosowany procesor musi wspierać standard PCIe Gen4.
22. Każdy kontroler musi posiadać co najmniej 192GB pamięci RAM o szybkości 3200MT/s.
23. Kontrolery muszą obsługiwać protokół iSCSI, FC, NVMeoF-FC na portach wystawionych do hostów (front-end).
24. Macierz musi być wyposażona, w co najmniej:
    a. 2 karty 2 portowe (po 1 karcie na kontroler) min. 32Gb FC wyposażone w min. 4 wkładki 32Gb SW (po 2 szt. na kontroler).
    b. 2 porty (po 1 na kontroler) Ethernet min. 1Gb BaseT do zarządzania macierzą
    c. 2 karty 2 portowe (po 1 karcie na kontroler) 10/25 Gb iSCSI muszą być we wszystkich portach obsadzone wkładkami 25Gb SFP28 Short Wave

25. Macierz musi zostać dostarczona z przewodami zasilającymi kompatybilnymi z infrastrukturą Zamawiającego. Zamawiający w udostępnionej przestrzeni szaf rack posiada złącza C13 i C19.
26. Zarządzanie macierzą dyskową musi być możliwe z poziomu interfejsu graficznego oraz linii poleceń.
27. Oprogramowanie do zarządzania musi pozwalać na stałe monitorowanie stanu macierzy oraz umożliwiać konfigurowanie jej zasobów dyskowych. Narzędzie musi pozwalać na obserwację danych wydajnościowych oraz prezentację ich w postaci wykresów oraz czytelnych raportów. Wymagane jest monitorowanie bieżących parametrów pracy macierzy.
28. Macierz musi zapewniać możliwość dynamicznego zwiększania pojemności wolumenów logicznych oraz wielkości grup dyskowych (przez dodanie dysków) z poziomu kontrolera macierzowego bez przerywania dostępu do danych.
29. 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.
30. Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie typu Thin Provisioning.
31. 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).
32. Macierz musi umożliwiać dokonywanie na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez konieczności wcześniejszego alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii.
33. Wymagany jest mechanizm Redirect-on-wite (ROW) lub równoważny, który nie wymaga kopiowania oryginalnych danych przy ich zmianie po wykonaniu migawki.
34. Macierz musi posiadać mechanizm uniemożliwiający jakiemukolwiek użytkownikowi (w tym administratorom) usunięcie migawkowej kopii danych przez zdefiniowany okres. Okres ten nie może zostać skrócony.
35. Macierz musi umożliwiać zdalną replikację danych typu online do innej macierzy z tej samej rodziny z wykorzystaniem protokołu FC i IP. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. Musi istnieć możliwość jednoczesnej natywnej replikacji w trybach: synchronicznym i asynchronicznym za pośrednictwem różnych infrastruktur (FC i IP).
36. Oprogramowanie musi zapewniać funkcjonalność zawieszania i ponownej przyrostowej resynchronizacji kopii z oryginałem oraz zamiany ról oryginału i kopii (dla określonej pary wolumenów logicznych) z poziomu interfejsu administratora.
37. Macierz musi umożliwiać replikowanie danych synchronicznie z drugą taką macierzą i zapewniać – w przypadku awarii i całkowitej niedostępności jednej z macierzy – ciągłą pracę systemów działających na platformie przetwarzania danych i korzystających z zasobów pamięci masowych. Opisane powyżej przełączenie między macierzami musi odbywać się w sposób automatyczny i transparentny dla korzystających z dysków logicznych macierzy serwerów i aplikacji. Opisana funkcjonalność musi zapewniać integrację z co najmniej Microsoft Cluster Service oraz platformą wirtualizacyjną VMware (VMware vSphere Metro Storage Cluster).
38. Rozwiązanie musi umożliwiać hostom jednoczesny zapis do obu macierzy dla tego samego wolumenu.
39. Macierz musi umożliwiać konfigurację gwarancji wydajności typu QoS w postaci ustawień kilku poziomów priorytetów obsługi.
40. Oferowana macierz musi umożliwiać definiowanie polityk Quality of Service na podstawie następujących algorytmów z możliwością przypisania do hosta lub grupy hostów.:
    a. Względne polityki wydajnościowe - definicja minimum trzech poziomów profili wydajnościowych
    b. Bezwzględne polityki wydajnościowe - definicja na podstawie ilości IOPS oraz MB/s.
    c. Bezwzględne polityki wydajnościowe - definicja na podstawie ilości IOPS oraz MB/s w przeliczeniu na wskazaną ilość danych w GB.
    d. Bezwzględne polityki wydajnościowe - definicja na podstawie ilości IOPS oraz MB/s z możliwością warunkowego przekroczenia limitu o zadaną wielkość wyrażoną w procentach ustawionego limitu.
    e. Zamawiający dopuszcza spełniającą wymagania macierz, która zamiast możliwości ustawiania poziomów priorytetów zapewnia konfigurację wydajności typu QoS poprzez definiowanie dla wolumenów maksymalnej przepustowości (kB/s) i wydajności IOPS
41. Macierz musi zapewniać kompresję i deduplikację danych na poziomie blokowym. Musi istnieć możliwość uruchomienia deduplikacji na poziomie pojedynczych wolumenów logicznych. Kompresja i deduplikacja nie mogą być realizowane za pomocą zewnętrznego urządzenia lub oprogramowania.

42. Mechanizmy kompresji i dedpuplikacji muszą być przezroczyste dla administratora macierzy.
43. Proces deduplikacji musi odbywać się globalnie (minimum w ramach pary kontrolerów).
44. Wobec powyższych wymagań dla każdego wolumenu macierzy musi zachodzić jednocześnie kompresja i deduplikacja danych, która nie wymaga konfiguracji ani żadnej innej interwencji ze strony administratora macierzy. Operacje kompresji i deduplikacji muszą działać na wszystkich rodzajach dostarczanych i opcjonalnych nośników SSD i być dostępne dla wszystkich rodzajów przechowywanych danych (nie jest dozwolone oferowanie rozwiązań, które nie zapewniłyby kompresji i deduplikacji na całej wymaganej pojemności).
45. Redukcja danych musi być wspierana przez dedykowany układ sprzętowy poza procesorem kontrolera macierzy.
46. Mechanizmy redukcji danych muszą być realizowane za pomocą zmiennego bloku, aby zapewnić maksymalną skuteczność tych procesów.
47. Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami).
48. Macierz musi wspierać podłączenie następujących systemów operacyjnych dla protokołu FC: Windows Server 2022, Red Hat 9.x, VMware 7.x, SLES 15 lub nowsze
49. Macierz musi wspierać podłączenie następujących systemów operacyjnych dla protokołu NVMeoF-FC: Red Hat 9.x, VMware 7.x lub nowsze.
50. 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.
51. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap", a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory.
52. Macierz musi mieć możliwość zasilania z dwóch niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.
53. Macierz musi umożliwiać wykonywanie aktualizacji mikrokodu macierzy w trybie online bez wyłączania żadnego z interfejsów macierzy
54. Zamawiający dopuszcza rozwiązanie za spełniającą wymagania macierz, która umożliwia wykonywanie aktualizacji mikrokodu macierzy w trybie online, czyli bez konieczności zatrzymywania systemów/aplikacji pracujących na macierzy, nawet w przypadku, gdy konieczne jest zrestartowanie kontrolerów, w tym interfejsów sieciowych.
55. Macierz musi umożliwiać zdalne zarządzanie macierzą oraz automatyczne informowanie centrum serwisowego o awarii.
56. Producent macierzy musi gwarantować 100% dostępność do danych dla pojedynczej macierzy. Wymagane potwierdzenie na publicznej stronie producenta na żądanie Zamawiającego
57. Oferowana macierz dyskowa musi być fabrycznie nowa, wyprodukowana nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z oficjalnego kanału dystrybucyjnego producenta na rynek polski. Zamawiający zastrzega sobie, aby Wykonawca na żądanie Zamawiającego przedłożył oświadczenie Producenta oferowanego sprzętu, w języku polskim, potwierdzające pochodzenie sprzętu z autoryzowanego kanału sprzedaży z Polski.
58. Minimum 3-letnia gwarancja producenta w miejscu instalacji. Możliwość zgłoszenia awarii przez siedem dni w tygodniu, 24 godziny na dobę. Czas reakcji serwisu do 1 godz. usunięcie usterki do 6-ciu godzin.
59. Uszkodzone dyski macierzy pozostają u Zamawiającego.
60. W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy.
61. Gwarancja na sprzęt musi być dostarczona i realizowana przez organizację serwisową producenta sprzętu.
62. Razem z macierzą należy dostarczyć zestaw licencji dla 2 przełączników FC będących w posiadaniu Zamawiającego. Zestaw licencji powinien umożliwiać rozszerzenie o 8 dostępnych portów dla każdego z przełączników. Wraz z licencjami należy dostarczyć certyfikowane wkładki oraz okablowanie o długości 3 metrów. Dane przełączników poniżej. Czas gwarancji oraz wsparcia licencji powinien być tożsamy z czasem gwarancji oraz wsparcia dostarczanej macierzy. W ramach dostarczenia licencji Zamawiający dodatkowo wymaga:
    a. Dostarczenia licencji i prawidłowe zarejestrowanie go w ramach systemów gwarancyjnych producenta przełączników
    b. Aktywacja i konfiguracja licencji w ramach przełączników
    c. Podłączenie i konfiguracja dostarczonej macierzy do wskazanych przełączników wraz z konfiguracją przełączników SAN zgodnie z aktualną architekturą sieci SAN
    d. Aktualizacja dokumentacji konfiguracji przełączników
63. Model przełączników - HPE SN3600B
64. Nr. Produktu - R7R97A
65. Nr. Seryjne - CZC4429ZYJ (Switch 1), CZC4429ZZW (Switch 2)

VIII. MINIMALNE WYMAGANIA TECHNICZNE I FUNKCJONALNE PRZEŁĄCZNIKÓW FIBRE CHANNEL

1. Przełącznik Fibre Channel musi mieć wysokość maksymalnie 1U (jednostka wysokości szafy montażowej) i zapewniać techniczną możliwość montażu w szafie 19”
2. Przełącznik FC musi być wykonany w technologii Brocade FC 16 Gb/s oraz 32 Gb/s i zapewniać możliwość pracy portów FC z prędkościami 32, 16, 8, 4 Gb/s w zależności od rodzaju zastosowanych wkładek SFP.
   a. W przypadku obsadzenia portu FC za pomocą wkładki SFP 16Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 16, 8 lub 4 Gb/s, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji
   b. W przypadku obsadzenia portu FC za pomocą wkładki SFP 8Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 8 lub 4 Gb/s, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji
   c. Wszystkie zaoferowane porty przełącznika FC muszą umożliwiać działanie bez tzw. Oversubscrypcji, gdzie wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika wyposażonej we wkładki 32Gbs mogą pracować równocześnie z pełną prędkością 32Gb/s.
   d. Całkowita przepustowość przełącznika FC dostępna dla maksymalnie rozbudowanej konfiguracji (24 porty) wyposażonej we wkładki 32Gbs musi wynosić minimum 768 Gb/s end-to-end.
3. Ilość i rodzaj portów Fibre Channel:
   a. Przełącznik Fibre Channel musi być wyposażony, w co najmniej 8 aktywnych portów FC obsadzone 8 wkładkami SFP+, wielomodowymi, krótkodystansowymi, ze złączem LC o prędkości 32 Gbit każda.
   b. Wszystkie dostarczone wkładki muszą być oryginalne, tj. dostarczane przez producenta oferowanego przełącznika, lub certyfikowane przez producenta oferowanego przełącznika do pracy z oferowanym modelem przełącznika, co oznacza, że dostarczony model wkładki musi znajdować się w ofercie sprzedaży producenta przełącznika lub na oficjalnej opublikowanej przez producenta przełącznika liście kompatybilności.
   c. Niedopuszczalne jest dostarczenie zamiennych wkładek niecertyfikowanych, których montaż mógłby spowodować utratę gwarancji producenta przełącznika lub jakiekolwiek problemy konfiguracyjne
4. Typ portów
   a. Możliwość konfiguracji portów typu: D_Port, E_Port, ,F_Port, M_Port; Przełącznik musi mieć obsługę trybu NPIV na portach
   b. Oczekiwana wartość opóźnienia przy przesyłaniu ramek FC między dowolnymi portami przełącznika nie może być większa niż 900ns.
5. Przełącznik Fibre Channel musi mieć możliwość wymiany i aktywacji wersji firmware’u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia i bez zakłócenia przesyłanego ruchu FC
6. Przełącznik Fibre Channel musi wspierać następujące mechanizmy zwiększające poziom bezpieczeństwa:
   a. mechanizm tzw. Switch Binding, który umożliwia zdefiniowanie listy kontroli dostępu regulującej prawa urządzeń FC do podłączenia do przełącznika fabric
   b. mechanizm tzw. Port Binding, który umożliwia zdefiniowanie listy kontroli dostępu regulującej prawa hostów i urządzeń storage FC do podłączenia do portu przełącznika
   c. uwierzytelnianie (autentykacja) przełączników w sieci Fabric za pomocą protokołów FCAP
   d. uwierzytelnianie (autentykacja) urządzeń końcowych w sieci Fabric za pomocą protokołu DH-CHAP
   e. szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2.
   f. definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control)
   g. definiowane kont administratorów w środowisku RADIUS, LDAP w MS Active Directory, Open LDAP, TACACS+
   h. szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS
   i. obsługa SNMP v1 oraz v3
   j. wgrywanie nowych wersji firmware przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP
   k. wykonywanie kopii bezpieczeństwa konfiguracji przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP
7. Przełącznik Fibre Channel musi umożliwiać rozbudowę o agregację połączeń ISL między dwoma przełącznikami i tworzenia w ten sposób logicznych połączeń typu trunk o przepustowości minimum 128 Gb/s half duplex dla każdego logicznego połączenia. Load balancing ruchu między fizycznymi połączeniami ISL w ramach połączenia logicznego typu trunk musi być realizowany na poziomie pojedynczych ramek FC a połączenie logiczne musi zachowywać kolejność przesyłanych ramek.

8. Przełącznik Fibre Channel musi realizować sprzętową obsługę zoningu (przez tzw. układ ASIC) na podstawie portów i adresów WWN.
9. Przełącznik Fibre Channel musi umożliwiać rozbudowę instalacji wkładek SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 25km z prędkością 16Gb/s.
10. Wsparcie dla N_Port ID Virtualization (NPIV). Obsługa, co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika
11. Przełącznik Fibre Channel musi mieć możliwość konfiguracji przez:
    a. HTTP/HTTPS, poprzez SSH, obsługa SNMP v1/v3,
    b. możliwość wysyłania logów na zewnętrzny serwer syslog,
    c. Osobny interfejs sieciowy 10/100/1000 Mbps Ethernet RJ-45 pozwalający na zarządzanie przełącznikiem
    d. Port szeregowy (RJ-45) pozwalający na bezpośrednie podłączenie się do przełącznika
12. Możliwość rozbudowy w przyszłości o poniższe licencje (dla każdego przełącznika)
    a. Fabric Vision
    b. ISL Trunking
    c. Extended Fabric
13. Możliwość diagnozowania z poziomu przełącznika połączeń światłowodowych, Możliwość pomiaru połączenia (prędkość, opóźnienia, dystans), wbudowany generator przepływu danych, możliwość wykonywania poleceń FC ping, Pathinfo (FCtraceroute), możliwość podglądu ramek, monitorowanie stanu łącz, monitorowanie stanu urządzenia
14. Preferowany sposób montażu i kierunek przepływu chłodnego powietrza
    a. Montaż w tylnej części szafy rack
    b. Przepływ powietrza chłodzącego przez przełącznik od tyłu urządzenia w kierunku interfejsów.
    c. Wraz z przełącznikiem wymagane jest dostarczenie wszelkich elementów i akcesoriów niezbędnych do prawidłowego zamontowania przełącznika w szafie RACK oraz prawidłowej cyrkulacji powietrza (np. szyny montażowe, śruby itp.)
15. Urządzenie musi współpracować z krajową siecią energetyczną o parametrach znamionowych: 230 V, 50 Hz.
16. Maksymalny dopuszczalny pobór mocy przełącznika FC wyposażonego w 24 aktywne porty 32Gbps to 77W.
17. Chłodzenie aktywne, zapewnione działanie urządzenia przy 2 uszkodzonych wentylatorach.
18. Oferowane produkty (urządzenia, sprzęt) muszą spełniać wymagania norm CE, tj. muszą spełniać wymogi niezbędne do oznaczenia produktów znakiem CE
19. Urządzenia i ich komponenty muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
20. Przełączniki sieci SAN muszą być nowe, nigdy wcześniej nie używane i pochodzić z autoryzowanego kanału dystrybucji producenta na terenie Polski a także być objęta serwisem producenta.
21. Wymagana jest gwarancja na wszystkie elementy przełącznika sieci SAN (sprzęt oraz oprogramowanie) na okres min. 60 miesięcy
22. Wraz z każdym przełącznikiem należy dostarczyć 8 szt. okablowania OM4 o długości minimum 5 metrów

IX. MINIMALNE WYMAGANIA w ZAKRESIE WDROŻENIA SYSTEMU WRAZ Z PRZEPROWADZENIEM INSTRUKTAŻU

1. Dostarczenie i instalacja platformy wirtualizacji będzie realizowana w 2 wskazanych lokalizacjach. Sprzęt będący przedmiotem niniejszego zamówienia zostanie dostarczony do dwóch lokalizacji wskazanej przez Zamawiającego znajdujących się na terenie Polski.
2. Dostarczenie platformy obejmuje dostawę wszelkich wymaganych do działania platformy oprogramowania oraz licencji/subskrypcji.
3. Konfigurację i uruchomienie urządzeń/elementów platformy wirtualizującej w środowisku Zamawiającego w terminie do 40 dni od podpisania umowy.
4. Wykonawca przeprowadzi instalację i konfigurację wszystkich elementów dostarczonej platformy wymaganą przez Zamawiającego.
5. Wszelkie prace konfiguracyjne muszą uwzględniać dobre praktyki i rekomendacje eksploatacyjne publikowane przez producenta dostarczonej infrastruktury sprzętowej oraz programowej.
6. Wdrożone klastry wirtualizacyjne muszą być skonfigurowane tak, aby był w pełni funkcjonalny we wszystkich czterech aspektach: serwerowym, dyskowym, sieciowym i zarządzania.
7. Przed rozpoczęciem prac należy ustalić plan adresacji sieci IP. Ustalenia te będą prowadzone z wyznaczonym do tego celu pracownikiem/pracownikami Zamawiającego.
8. Zamawiający zapewni przestrzeń min. 15U w szafie RACK 19”, zasilanie gwarantowane wraz z niezbędną ilością gniazd w listwach zasilających dla obydwu lokalizacji.

9. Zamawiający zapewni niezbędną ilość portów w standardzie 1000BASE-T na potrzeby zarządzania dostarczonym środowiskiem.
10. Prace wdrożeniowe klastra wirtualizacyjnego będą polegały w szczególności na:
    a. montażu i podłączeniu fizycznym sprzętu w serwerowni (szafa RACK wskazana przez zamawiającego),
    b. podłączeniu zasilania oraz sieci management,
    c. aktualizacji oprogramowania układowego i jego komponentów wszystkich dostarczonych komponentów,
    d. konfiguracji macierzy dyskowej, przełączników sieciowych,
    e. hardeningu urządzeń oraz wdrażanego oprogramowania według najlepszych praktyk producenta,
    f. niezbędnej rekonfiguracji istniejącej infrastruktury informatycznej (VLANY, routing, polityki firewalla, wpisy DNS),
    g. aktywacji zakupionego oprogramowania oraz wszelkich subskrypcji i serwisów producenta,
    h. konfiguracji oraz uruchomieniu klastra wirtualizacyjnego, opartego o dostarczane oprogramowanie witrualizacyjne.
11. Wykonaniu testów akceptacyjnych (niezawodnościowe oraz funkcjonalne) oraz opracowaniu i przedstawieniu Raport z testów Wykonanie dokumentacji powykonawczej wszystkich wdrożonych elementów.
12. Dokumentacja powykonawcza, musi w szczególności zawierać następujące elementy:
    a. architektury logicznej,
    b. architektury fizycznej,
    c. architektury sieciowej,
    d. konfiguracji klastra wirtualizacyjnego, zasobów dyskowych i sieci,
    e. zestawienie wersji firmware zainstalowanych na dostarczonych urządzeniach,
    f. zestawienie zakupionego i aktywowanego oprogramowania,
    g. specyfikacja techniczna dostarczonego sprzętu,
    h. schemat rozmieszczenia zainstalowanych urządzeń w szafach RACK i fizycznymi połączeniami między nimi,
    i. tabele wykorzystanych adresów IP
    j. zebrane informacje na temat obsługi wsparcia dostarczonych urządzeń, adresy url, nazwy kont do logowania, numery telefonów, adresy e-mail
13. Przeprowadzenie instruktażu
14. Wykonawca przeprowadzi instruktaż dla administratorów wskazanych przez Zamawiającego:
    a) Instruktaż zostanie przeprowadzony w terminie uzgodnionym z Zamawiającym (jednak nie później niż 10 dni od daty wdrożenia), w jego siedzibie, tj. Plac Trzech Krzyży 3/5, 00-507 Warszawa.
    Instruktaż powinien obejmować:
    b) omówienie dostarczonego sprzętu i oprogramowania (parametry, funkcjonalności),
    c) omówienie przeprowadzonych prac instalacyjno-konfiguracyjnych,
    d) omówienie i weryfikację przygotowanych i dostarczonych procedur,
    e) omówienie scenariuszy w przypadku wystąpienia błędów/awarii.

    Przed ustalonym terminem instruktażu Wykonawca prześle Zamawiającemu zakres tematyczny/programu instruktażu. Zamawiający będzie miał prawo do weryfikacji zakresu tematycznego/programu instruktażu i zgłoszenia ew. dodatkowego zakresu tematycznego.

X. MINIMALNE WYMAGANIA W ZAKRESIE GWARANCJI

Gwarancja dla oferowanych urządzeń i oprogramowania musi spełniać niżej opisane wymagania:

1. Minimalny okres gwarancji na urządzenia i oprogramowanie wskazany w Formularzu Ofertowym
2. Zamawiający wymaga, aby usługa gwarancyjna na wszystkie dostarczone w ramach zamówienia sprzęt była, przez cały okres jej trwania, świadczona na podstawie wykupionego wsparcia producenta dostarczonych urządzeń, to jest by zapewniona była naprawa lub wymiana urządzeń lub ich części, na części nowe i oryginalne, zgodnie z metodyką i zaleceniami producenta dostarczanego urządzeń i był jego autoryzowanym dostawcą.
3. Wszystkie urządzenia dostarczone i zastosowane przez Wykonawcę będą pochodziły z autoryzowanego kanału sprzedaży producentów Urządzeń na rynek polski lub Unii Europejskiej. Spełnienie powyższego wymogu zostanie potwierdzone oświadczeniem producenta Urządzeń

lub jego polskiego przedstawicielstwa, które Wykonawca zobowiązuje się dostarczyć Zamawiającemu najpóźniej w dniu dostawy oferowanych Urządzeń.

4. Gwarancja będzie liczona od daty odbioru przedmiotu umowy i oparta na gwarancji producentów rozwiązania. Serwis gwarancyjny świadczony ma być w miejscu instalacji Sprzętów.
5. Gwarancja ma być świadczona w reżimie 8x5xNBD. Czas naprawy Awarii liczony jest od czasu przesłania zgłoszenia o awarii do Wykonawcy zgodnie z procedurą przyjmowania zgłoszeń serwisowych.
6. Zamawiający dopuszcza świadczenie serwisu dla dostarczonych urządzeń poprzez zastosowanie zamienników wskazanych przez producenta tylko i wyłącznie w przypadku, gdy takiego wsparcia u producenta nie da się wykupić (np. produkty zostały wycofane przez producenta bez możliwości świadczenia serwisu).
7. W przypadku, gdy w okresie gwarancyjnym nastąpi trzykrotna naprawa wadliwego podzespołu Wykonawca niezwłocznie tj. w terminie nie dłuższym niż 14 dni liczonych od dnia zgłoszenia awarii, dokona jego wymiany na sprzęt nowy, wolny od wad. Na czas potrzebny do wymiany podzespołu wykonawca dostarczy element zastępczy o parametrach tożsamych z podzespołem uszkodzonym. Zamawiający oczekuje, iż w wypadku konieczności wymiany urządzenia, dyski na których zapisane są dane nieulotne wymienianego urządzenia pozostaną w siedzibie Zamawiającego.
8. Zamawiający otrzyma dostęp do pomocy technicznej Wykonawcy (telefon, e-mail lub www) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych urządzeń w godzinach pracy Zamawiającego.
9. Zamawiający zastrzega sobie prawo do dodawania nowych modułów oraz wymiany zainstalowanych modułów samodzielnie lub z pomocą Wykonawcy, w zakresie przewidzianym przez producenta Urządzenia, bez utraty gwarancji na zakupione Urządzenia. Zamawiający będzie dokonywał wymiany modułów samodzielnie po wcześniejszym uzgodnieniu z Wykonawcą. W przypadku nieprawidłowego lub niezgodnego z zaleceniami Wykonawcy i producenta Urządzenia dodania modułów lub wymiany zainstalowanych modułów przez Zamawiającego Wykonawca nie jest obciążony gwarancją i rękojmią w tym zakresie.
10. W okresie gwarancji Wykonawca w ramach otrzymanego wynagrodzenia udostępni Zamawiającemu możliwość wielokrotnego uaktualniania całego dostarczonego Oprogramowania do najnowszych wersji oferowanych przez producenta (włączając tzw. firmware) oraz patche i programy korekcji błędów, a także dostęp do usług wsparcia technicznego producenta właściwy dla danego Urządzenia lub Oprogramowania. W przypadku, gdy dostęp taki wymaga podania nazwy użytkownika, hasła lub numeru seryjnego Wykonawca dostarczy Zamawiającemu ww. przed podpisaniem protokołu odbioru Urządzeń.
11. W przypadku konieczności naprawy Urządzenia lub Oprogramowania poza Lokalizacją, Wykonawca pokrywa koszty transportu i ponosi ryzyko uszkodzenia lub przypadkowej utraty urządzenia lub oprogramowania Standardowego w przypadku konieczności naprawy poza siedzibą Zamawiającego.
12. Na okres przedłużającej się naprawy Wykonawca może stosować procedury zastępcze. Czas trwania procedur zastępczych nie może być dłuższy niż 45 dni kalendarzowe od chwili zgłoszenia awarii.
13. Przez usunięcie Awarii należy rozumieć przywrócenie pierwotnej funkcjonalności Systemu we wszystkich modułach i zaprzestanie stosowania w bieżącej prac rezerwowego Urządzenia i/lub procedur zastępczych.
14. Po usunięciu każdej Awarii, Wykonawca zobowiązuje się do doprowadzenia całego systemu do stanu integralnej całości w rozumieniu poprawnego działania wszystkich zainstalowanych komponentów.
15. W ramach gwarancji Zamawiający będzie miał prawo przez okres wskazany w formularzu ofertowym do:
    a) pobierania i instalowania nowych wersji oprogramowania dla każdego elementu wchodzącego w skład oferty
    b) Dostępu do bazy wiedzy oraz dokumentacji dostarczonych elementów
    c) Dostępu do powiadomień/ogłoszeń/alarmów w zakresie dostarczonych elementów
    d) Zgłaszania nieograniczonej liczby awarii systemu w trybie 24x365x7 za pomocą dedykowanego portalu i/lub zgłoszenia telefonicznego,
    e) Wymiany uszkodzonych/wadliwych dostarczonych elementów w trybie NDB (Next-Bussines Day),
16. Czasy reakcji/naprawy na zgłoszenie będą na poziomie:

a) 1 godzina/8 godzin - błąd krytyczny – tj. przerwa w działaniu usług w środowisku produkcyjnym, brak dostępnego obejścia problemu,

b) 2 godziny/2 dni - błędy wysokie – tj. problem z poprawnym działaniem usługi znacząco utrudniający realizację procesów biznesowych, brak dostępnego obejścia problemu,

c) 4 godziny/7 dni - błędy średnie - tj. problem z poprawnym działaniem usługi, utrudnienie realizacji procesów biznesowych, dostępne obejście problemu,

d) 8 godzin/14 dni - błędy niskie – tj. problem z poprawnym działaniem usługi, brak wpływu na realizację procesów biznesowych.

17. Wykonawca do dostarczonych urządzeń, będących przedmiotem zamówienia, dołączy karty gwarancyjne zawierające numer seryjny, termin i warunki ważności gwarancji, adresy i numery telefonów punktów serwisowych świadczących usługi gwarancyjnej.
18. Wykonawca w terminie 7 dni od zawarcia Umowy dostarczy Zamawiającemu procedury zgłaszania i obsługi Awarii wraz z listą osób upoważnionych do kontaktów, wykazem adresów poczty elektronicznej i nr telefonów.
19. Wykonawca, najpóźniej w dniu zawarcia Umowy, przedstawi do akceptacji Zamawiającemu listę osób uprawnionych do wykonywania czynności serwisowych.
20. W okresie gwarancji Wykonawca ponosi odpowiedzialność za poprawne funkcjonowanie urządzeń i oprogramowania stanowiącego przedmiot zamówienia, z zastrzeżeniem, że Wykonawca nie ponosi odpowiedzialności za uszkodzenia urządzeń i oprogramowania powstałych z wyłącznej winy Zamawiającego lub osób trzecich działających w jego imieniu.
21. Wymagany tryb zgłaszania wszelkich awarii, wad i błędów. Zgłoszenie następuje w drodze pisemnej mailem na adres podany przez Wykonawcę lub za pośrednictwem telefonicznego zgłaszania awarii, wad i błędów dotyczących sprzętu i oprogramowania w dni robocze w godzinach 8:00-17:00.
22. Zamawiający wymaga obsługi zgłoszeń w języku polskim.