Szczegółowy opis przedmiotu zamówienia

1. Serwer rack na potrzeby rozbudowy infrastruktury hiperkonwergentnej (HCI) - 3 szt. w ramach zamówienia gwarantowanego oraz do 2 szt. w ramach realizacji zamówienia opcjonalnego.

Lp.	Konfiguracja minimalna Zamawiającego	
1.	Moduł TPM	W wersji minimum 2.0.
2.	Obudowa	Obudowa Rack o wysokości max 2U z możliwością instalacji do min. 24 dysków 2,5 cala. Komplet szyn umożliwiających montaż w szafie rack z możliwością wysuwania podczas pracy z wysuwanym ramieniem z organizatorem kabli. Minimum 4 porty PCIe Full Height.
3.	Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
4.	Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
5.	Procesor	Jeden procesor trzydziestodwu-rdzeniowy klasy x86 dedykowany do pracy z zaoferowanym serwerem, 64 wątki, minimum 48 MB Cache, minimum 2.6 GHz, kompatybilny z posiadanym środowiskiem przez Zamawiającego z uruchomionym VMware EVC mode Intel "Broadwell" Generation.
6.	Pamięć RAM	1024 GB DDR4 min. 3200 MT/s, na płycie głównej musi znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Jedna kość RAM minimum 128 GB.
7.	Gniazda PCI	Minimum 3 sloty PCIe x8 generacji 3 lub generacji 4 oraz minimum 1 slot PCIe x16 generacji 3 lub generacji 4
8.	Interfejsy Sieciowe	Dwa interfejsy sieciowe 1 Gb Ethernet w standardzie BaseT oraz cztery interfejsy sieciowe 10/25 Gb Ethernet ze złączami w standardzie SFP28 kompatybilne z wkładkami SFP+.
9.	Dyski twarde	4 dyski min. 400 GB SSD 2,5” min. 6 DWPD 20 dysków min. 3.84 TB SSD 2.5” min. 1 DWPD. Dyski muszą być z kieszeniami zainstalowane w serwerze, kompatybilność z VMware vSAN w wersji 7.0 lub wyższej.
10.	Kable	4 kable SFP+ (DAC) 5m, kompatybilne z serwerem i VMware w wersji 7.0.
11.	Kontroler dysków	Sprzętowy kontroler dyskowy typu HBA obsługujący tryb Pass-Through oraz vSAN Secure-wipe capable dla konfiguracji All-Flash. Wsparcie dla min. 24 dysków, kompatybilność z VMware vSAN

		w wersji 6.7U3, 7.0U3 oraz 8. Kontroler musi znajdować się na liście VMware Compatibility Guide: https://www.vmware.com/resources/compatibility/search.php
12.	Wbudowane porty	min. 1 port USB 2.0, 2 porty USB 3.0, 1 port VGA lub HDMI lub DisplayPort.
13.	Video	Zintegrowana karta graficzna.
14.	Wentylatory	Minimum 6 sztuk wewnątrz obudowy.
15.	Zasilanie	Serwer musi być wyposażony w minimum dwa zasilacze o mocy minimalnej 1100 W każdy, pozwalające na jednoczesne zasilanie z minimum dwóch niezależnych źródeł zasilania. Wymiana zasilacza musi być możliwa bezprzerwowo (hot-plug).
16.	Bezpieczeństwo	Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
17.	Panel	Przedni panel obudowy zdejmowalny, zamykany na kluczyk umożliwiający zakrycie dysków, chroniący dyski przed przypadkowym wyjęciem.
18.	Zarządzanie	1. Niezależna od zainstalowanego na serwerze systemu operacyjnego karta zarządzająca posiadająca dedykowany port RJ-45 Gigabit Ethernet umożliwiająca: 1) zdalny dostęp do graficznego interfejsu Web karty zarządzającej; 2) zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); 3) szyfrowane połączenie (TLS 1.2) oraz autentykację i autoryzację użytkownika; 4) możliwość podmontowania zdalnych wirtualnych napędów; 5) wirtualną konsolę z dostępem do myszy, klawiatury; 6) wsparcie dla IPv6; 7) wsparcie dla SNMP; IPMI 2.0, VLAN tagging, Telnet, SSH; 8) możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; 9) zdalne ustawienia limitu poboru prądu przez konkretny serwer; 10) integrację z Active Directory; 11) obsługę przez dwóch administratorów jednocześnie; 12) wsparcie dla dynamic DNS; 13) wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej; 14) Producent systemu musi posiadać dedykowane

		rozwiązanie które będzie przeciwdziałało automatycznym skryptom konfiguracyjnym działającym w sieci. Jest niedopuszczalne aby konsole zarządzające serwerów miały identyczne dane dostępowe; 15) możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy; 16) możliwość konfiguracji przepływu powietrza na każdym slocie PCIe, jak również musi posiadać możliwość konfiguracji wyłączania lub włączania poszczególnych wentylatorów; 17) możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi; 18) możliwość zablokowania konfiguracji oraz odnowienia oprogramowania karty zarządzającej poprzez jednego z administratorów. Podczas trwania blokady musi być ona wyświetlana dla wszystkich administratorów którzy obecnie korzystają z karty; 19) polaczenie do konsoli zarządzającej nie może wymagać zainstalowania na kliencie żadnych pakietów Java. 2. Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania: 1) Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych; 2) Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta; 3) Wsparcie dla protokołów – WMI, SNMP, IPMI, , Linux SSH; 4) Możliwość oskryptowywania procesu wykrywania urządzeń; 5) Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram; 6) Szczegółowy opis wykrytych systemów oraz ich komponentów; 7) Możliwość eksportu raportu do CSV, HTML, XLS; 8) Grupowanie urządzeń w oparciu o kryteria użytkownika; 9) Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach; 10) Automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń; 11) Szybki podgląd stanu środowiska; 12) Podsumowanie stanu dla każdego urządzenia; 13) Szczegółowy status urządzenia /elementu/ komponentu; 14) Generowanie alertów przy zmianie stanu urządzenia; 15) Filtry raportów umożliwiające podgląd najważniejszych zdarzeń;

		16) Integracja z service desk producenta dostarczonej platformy sprzętowej; 17) Możliwość przejęcia zdalnego pulpitu; 18) Możliwość podmontowania wirtualnego napędu; 19) Automatyczne zaplanowanie akcji dla poszczególnych alertów w tym automatyczne tworzenie zgłoszeń serwisowych w oparciu o standardy przyjęte przez producentów oferowanego w tym postępowaniu sprzętu; 20) Kreator umożliwiający dostosowanie akcji dla wybranych alertów; 21) Możliwość importu plików MIB; 22) Przesyłanie alertów „as-is" do innych konsol firm trzecich; 23) Możliwość definiowania ról administratorów; 24) Możliwość zdalnej aktualizacji sterowników i oprogramowania wewnętrznego serwerów; 25) Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania); 26) Możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta; 27) Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów; 28) 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 gwarancji, adresy IP kart sieciowych; 29) Możliwość automatycznego przywracania ustawień serwera, kart sieciowych, BIOS, wersji firmware w przypadku awarii i wymiany któregoś z komponentów (w tym kontrolera RAID, kart sieciowych, płyty głównej).
19.	Certyfikaty	Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów: Microsoft Windows Server 2016 x64, Microsoft Windows Server 2019 x64, Microsoft Windows Server 2022 x64.
20.	Gwarancja	7 (siedem) lat gwarancji producenta realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta/email lub portal producenta. W przypadku uszkodzenia nośnika danych (dysku), uszkodzony

		nośnik pozostaje u Zamawiającego.
21.	Dokumentacja	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego i/lub na stronie internetowej producenta sprzętu, sprawdzenia konfiguracji sprzętowej oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
22.	Wymagania dodatkowe	Wszystkie komponenty muszą być kompatybilne ze sobą. Wszystkie komponenty, w tym w szczególności dyski twarde, kontroler dysków, karty sieciowe wraz z kablami muszą być kompatybilne i działać w środowisku VMware vSAN w wersji minimum 7.0. Wszystkie ewentualne niewykorzystane sloty dysków twardych muszą być wyposażone w zaślepkę.
23.	Licencje na oprogramowanie	Microsoft Windows Server 2022 Datacenter - 16 Core License Pack - 2 szt. lub oprogramowanie równoważne; 1) licencja bezterminowa; 2) licencja pozwalająca na swobodne przenoszenie pomiędzy serwerami; 3) licencja zapewniająca możliwość korzystania z wcześniejszych wersji zamawianego oprogramowania i korzystania z kopii zamiennych; 4) dostęp do witryny producenta umożliwiający pobieranie kodu zamówionego oprogramowania i kluczy licencyjnych. Warunki równoważności dla serwerowego systemu operacyjnego (licencja na 32 rdzeni procesora): 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. Dodatkowo musi pozwalać na wykorzystanie tej licencji w usłudze hostowanej platformy producenta serwerowego systemu operacyjnego. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy: 1) Możliwość wykorzystania nielimitowanej liczby rdzenie logicznych procesorów oraz co najmniej 24 TB pamięci RAM w środowisku fizycznym. 2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz minimum 1TB pamięci RAM i dysku o pojemności minimum 64TB przez każdy wirtualny serwerowy system operacyjny. 3) Możliwość budowania klastrów składających się z 64 węzłów. 4) Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn

		wirtualnych wewnątrz zespołu. 5) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 6) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. 7) Wbudowane wsparcie instalacji i pracy na wolumenach, które: a) pozwalają na zmianę rozmiaru w czasie pracy systemu, b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d) umożliwiają zdefiniowanie list kontroli dostępu (ACL). 8) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 9) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 10) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 11) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 12) Możliwość wykorzystania standardu http/2. 13) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 14) Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 15) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 16) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 17) Mechanizmy logowania w oparciu o: a) Login i hasło, b) Karty z certyfikatami (smartcard), c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 18) 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. 19) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 20) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 21) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 22) Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 23) Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 24) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b) 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: – Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, – Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, – Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. – Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows. c) Zdalna dystrybucja oprogramowania na stacje robocze. d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników. e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: – Dystrybucję certyfikatów poprzez http – Konsolidację CA dla wielu lasów domeny, – Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, – Automatyczne występowanie i używanie

		(wystawianie) certyfikatów PKI X.509. f) Szyfrowanie plików i folderów. g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h) Szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi. i) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. j) Serwis udostępniania stron WWW z uruchomionym domyślnie TLS 1.3. k) Wsparcie dla protokołu IP w wersji 6 (IPv6), l) Wsparcie dla algorytmów Suite B (RFC 4869), m) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, n) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. o) Możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. p) Możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. q) Mechanizmy wirtualizacji mające wsparcie dla: – Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, – Obsługi ramek typu jumbo frames dla maszyn wirtualnych. – Obsługi 4-KB sektorów dysków – Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra – Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. – Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) – Możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego. 25) Możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów. 26) Wsparcie dla rozwiązania Kubernetes.

		27) 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. 28) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 29) Mechanizmy deduplikacji i kompresji na wolumenach do 64 TB. 30) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 31) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 32) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. 33) Mechanizm konfiguracji połączenia VPN do platformy Azure. 34) Wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu. 35) Mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów. 36) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.