Załącznik nr 1 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Zakup i dostawa serwera redundancji (bazodanowego, zarządzania użytkownikami, systemami i sieciami) **- liczba sztuk: 1**

   Producent: .....

   Model: .....

   Procesor .....

Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry techniczne
Obudowa	Obudowa Rack z możliwością instalacji min. 8 dysków 2.5” U.2 wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.	
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Obsługa procesorów min. 48 rdzeniowych. Na płycie głównej powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać minimum 1TB pamięci RAM.	
Procesor	Zainstalowane dwa procesory min. 12-rdzeniowe klasy x86, min. 2.0GHz, dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 216 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej	
RAM	Minimum 256 GB pamięci DDR5 RDIMM min. 5600MT/s	
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający: min. 8GB nieulotnej pamięci cache, możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60, wsparcie dla dysków samoszyfrujących	
Interfejsy sieciowe/FC/SAS	Wbudowane min. 1 interfejs sieciowy 1Gb Ethernet w standardzie BaseT 2 interfejsy sieciowe 40Gb lub 100Gb Ethernet	

	w standardzie SFP28 **Karta Fibre Channel 2 x 32Gb (FC32) + 2 kable światłowodowe o długości min. 3m**	
Dyski twarde	Zainstalowane: 2 x dyski M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1. 4 x dyski U.2 lub U.3 NVMe SSD o pojemności min. 3.84TB, Hot-Plug	
Wbudowane porty	4x USB, w tym min. 1 porty USB 3.0 2x port VGA (jeden na panelu przednim)	
Wentylatory	Redundantne, Hot-Plug	
Zasilacze	Redundantne, Hot-Plug min. 1100W klasy Titanium	
System operacyjny/dodatkowe oprogramowanie	Licencja na serwerowy system operacyjny, w wersji najnowszej oferowanej przez producenta musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na zaoferowanym serwerze. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy: 1) 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. 2) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 3) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.	

	4) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 5) 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). 6) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 7) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 8) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 9) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 10) 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. 11) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB,	

	Plug&Play). 12) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 13) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 14) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 15) 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: I. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, II. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, III. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. c) Zdalna dystrybucja oprogramowania na stacje robocze. d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej e) Centrum Certyfikatów (CA), obsługa klucza	

	publicznego i prywatnego) umożliwiające: I. Dystrybucję certyfikatów poprzez http II. Konsolidację CA dla wielu lasów domeny, III. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, IV. 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) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i) Serwis udostępniania stron WWW. j) Wsparcie dla protokołu IP w wersji 6 (IPv6), k) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie 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: I. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, II. Obsługi ramek typu jumbo frames dla maszyn wirtualnych. III. Obsługi 4-KB sektorów dysków IV. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra V. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.	

	VI. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 16) 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. 17) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.	
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 powinien mieć 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. Moduł TPM 2.0 Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera	
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: a) zdalny dostęp do graficznego interfejsu Web karty zarządzającej; b) zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);	

	c) szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; d) możliwość podmontowania zdalnych wirtualnych napędów; e) wirtualną konsolę z dostępem do myszy, klawiatury; f) wsparcie dla IPv6; g) wsparcie dla dynamic DNS; h) wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.	
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025.	
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.	
Warunki gwarancji	Min. 5 lat gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy (dla krytycznych zgłoszeń serwisowych) Zgłoszenie przyjęte jest potwierdzane przez	

	zespół pomocy technicznej przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy/ producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.	

2. Zakup i dostawa przełącznika sieciowego - liczba sztuk: 1

Producent: .....

Model: .....

Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry techniczne
Obudowa	rack 19” o wysokości max. 2U	
Liczba i rodzaj portów	min. 32 x RJ45 min. 10Gb/s, min. 16 RJ45 x porty 2.5 GbE min. 4 x porty 25G SFP28 **w tym 2 porty z zamontowanymi modułami optycznymi kompatybilnymi z SFP28 o krótkim zasięgu** (25 Gbps przepustowości, kompatybilny z SFP28, połączenie do 100 m)	
Przepustowość przełączania	min. 460 Gbps	

Obsługiwane standardy	ANSI/TIA-1057:, IEEE 802.1AB, IEEE 802.1D, IEEE 802.1S, IEEE 802.1Q, IEEE 802.1p, IEEE 802.1X, IEEE 802.3ac, IEEE 802.3ad, IEEE 802.3x	
Obsługiwane funkcjonalności	Port Security, co najmniej: Centralizowana konfiguracja VLAN, Spanning Tree, IGMP Snooping, L3 Routing, Virtual Domain, Policy-Based Routing, 802.1X Authentication, Obsługa Syslog, DHCP Snooping, MAC Filtering, Clients Monitoring, Application Control, sFlow, ACL, DHCP Relay, Port Mirroring, ECMP, BFD, WoL, zabezpieczenie przeciwko pętli, IGMP Snooping, Storm Control, Obsługa SNMP v3, RMON	
Zarządzanie	SSH, HTTPs	
Praca w warstwach	L2, L3	
Certyfikaty	Przełącznik sieciowy musi posiadać deklaracja CE	
Pozostałe	2 x Kabel światłowodowy o długości min. 3m	
Gwarancja producenta	Min. 2 lata	