

OPIS PRZEDMIOTU ZAMÓWIENIA

CZĘŚĆ 1:

Serwer do backup wraz z oprogramowaniem – Windows Server2025 Datacenter - 16 Core/ Licencja Wieczysta/ EDU - 1 szt.

1. Nazwa i siedziba Zamawiającego

Sieć Badawcza Łukasiewicz - Instytut Chemii Przemysłowej
imienia Profesora Ignacego Mościckiego w Warszawie
ul. Rydygiera 8, 01-793 Warszawa

Parametr	Charakterystyka (wymagania minimalne)
Narzędzie planowania infrastruktury	W ramach postępowania zamawiający wymaga dostarczenia następujących elementów oprogramowania w pełnych działających wersjach. Oferujący dostarczy lub wskaże oprogramowanie do planowania infrastruktury, które umożliwia szacowanie zużycia energii przez sprzęt IT, infrastrukturę zasilania oraz pamięć masową. Narzędzie powinno zapewniać: - możliwość dokładnej symulacji i kalkulacji zużycia energii przez różne konfiguracje sprzętowe, uwzględnianie wpływu obciążeń i trybów pracy na zużycie energii, - szacowanie kosztów energii w skali rocznej oraz obliczenia emisji CO2 związanej z eksploatacją infrastruktury, elastyczne ustawienia uwzględniające różne parametry środowiskowe i efektywność zasilania (np. wskaźnik PUE), - łatwą obsługę przez użytkownika i generowanie raportów planistycznych wspierających optymalizację infrastruktury pod kątem efektywności energetycznej.
Oprogramowanie do centralnego zarządzania	Oferujący dostarczy lub wskaże oprogramowanie do centralnego zarządzania infrastrukturą serwerową, pamięcią masową oraz urządzeniami sieciowymi, które: - Umożliwia scentralizowany, intuicyjny w obsłudze widok i zarządzanie urządzeniami w ramach całej infrastruktury IT. - Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych. - Możliwość zarządzania dostarczonymi serwerami bez konieczności instalacji dedykowanego agenta (agentless), z obsługą takich protokołów jak WMI, SNMP, IPMI, WSMAN oraz Linux SSH. - Funkcje umożliwiające oskryptowywanie procesu wykrywania urządzeń. - Możliwość harmonogramowania procesu wykrywania urządzeń, w tym uruchamiania go o określonych godzinach i z określoną częstotliwością. - Szczegółowy opis wykrytych systemów oraz ich komponentów. - Eksport raportów w formatach CSV, HTML oraz XLS(X). - Grupowanie urządzeń według kryteriów definiowanych przez użytkownika, z możliwością automatycznego dodawania i edycji grup za pomocą skryptów CLI. - Szybki i przejrzysty podgląd stanu całego środowiska oraz podsumowanie stanu dla każdego urządzenia. - Wyświetlanie szczegółowego statusu urządzenia, jego elementów i komponentów. - Generowanie alertów w momencie zmiany stanu urządzenia oraz możliwość filtrowania raportów pod kątem najważniejszych zdarzeń. - Integracja z systemem helpdesk producenta dostarczonej platformy sprzętowej.

	- Możliwość przejęcia zdalnego pulpitu oraz podmontowania wirtualnego napędu. - Kreator umożliwiający definiowanie i dostosowanie działań podejmowanych w reakcji na wybrane alerty. - Możliwość importu plików MIB w celu rozbudowy funkcji monitoringu. - Przesyłanie alertów w formacie niezmienionym („as-is”) do konsol innych firm. - Mechanizmy aktualizacji oprogramowania, bazujące na wyborze źródła bibliotek (lokalnych lub on-line od producenta rozwiązania). - Możliwość instalacji sterowników i oprogramowania wewnętrznego (firmware) bez potrzeby instalacji agenta. - Możliwość tworzenia ról administratorskich z różnym poziomem uprawnień, na przykład roli dedykowanej wyłącznie do aktualizacji oprogramowania układowego. - Funkcjonalność automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta sprzętu. - Moduł raportujący pozwalający wygenerować szczegółowe informacje dotyczące numerów seryjnych sprzętu, konfiguracji urządzeń, wersji oprogramowania wewnętrznego, obsadzenia slotów PCIe i gniazd pamięci RAM, informacji o maszynach wirtualnych, aktualnym stanie gwarancji oraz adresach IP kart sieciowych
Oprogramowanie do zarządzania wsparciem produktu	Oferujący dostarczy lub wskaże oprogramowanie do zarządzania wsparciem producenta połączone z oficjalnym działem wsparcia technicznego, automatycznie tworzące zgłoszenia serwisowe w przypadku awarii. Zgłoszenia serwisowe zgłaszane przez aplikację muszą być traktowane na równi z tradycyjnym zgłoszeniem serwisowym przez dział techniczny producenta serwera. Oprogramowanie powinno być dostępne w postaci aplikacji na systemy Windows lub linux lub w postaci maszyny wirtualnej potrafiącej obsłużyć jednocześnie wiele serwerów. Konfiguracja i zaoferowany poziom wsparcia powinien po wystąpieniu awarii urządzenia automatycznie zakładać zlecenie serwisowe w dziale wsparcia producenta, poinformować o tym za pomocą wiadomości e-mail, a następnie dział wsparcia powinien się kontaktować z klientem w celu rozwiązania problemu. Oprogramowanie musi współpracować z kartą do zarządzania w urządzeniu, która będzie działać niezależnie od zainstalowanego systemu operacyjnego, posiadająca dedykowane port RJ-45 Gigabit. Karta musi umożliwiać podmontowanie zdalnych wirtualnych napędów oraz wirtualną konsolę z dostępem do myszy, klawiatury. Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające: - Proaktywne, zautomatyzowane wykrywanie problemów, tworzenie zgłoszeń i wysyłanie powiadomień. - Predykcyjna analiza i wykrywanie awarii dysków twardych i płyt głównych serwerów. - Szybsze rozwiązywanie problemów dzięki zdalnemu dostępowi i bezpiecznej dwukierunkowej komunikacji między serwisem producenta serwera, a środowiskiem klienta. - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS’u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji:

	• poprawkach i usprawnieniach dotyczących aktualizacji • dacie wydania ostatniej aktualizacji • priorytecie aktualizacji • zgodność z systemami operacyjnymi • jakiego komponentu sprzętu dotyczy aktualizacja • wszystkie poprzednie aktualizacje z informacjami jak powyżej • wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne • możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga. • rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr) • sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania) • - dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml • raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach, zainstalowanych aktualizacjach z dokładnym rozbiorem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku .xml od razu spakowany z rozszerzeniem .zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.
Oprogramowanie do centralnego monitorowania	Oferujący dostarczy lub wskaże w pełni funkcjonalne oprogramowanie do centralnego monitorowania umożliwiające proaktywne monitorowanie oraz rozwiązywanie problemów w infrastrukturze IT. Platforma powinna spełniać poniższe wymagania funkcjonalne: - Monitoring - System powinien zapewniać kompleksową obserwację środowiska IT z dostępem do: - liczby podłączonych i odłączonych systemów, - aktualnego stanu wszystkich urządzeń, - szczegółowych informacji o zagrożeniach cyberbezpieczeństwa (uwzględniających dobre praktyki oraz analizę istniejących systemów), - alertów z podziałem co najmniej na: krytyczne, błędy i ostrzeżenia, - statusu gwarancji dla poszczególnych urządzeń, - stanu licencji na wszystkie elementy rozszerzające funkcjonalność, - analizy danych historycznych pozwalających przewidywać trendy i zużycie pamięci masowych w ujęciu krótko- i długoterminowym, - wykrywania anomalii w wykorzystaniu przestrzeni dyskowej, - identyfikacji problemów wydajnościowych na podstawie uczenia maszynowego (z porównaniem bieżących i historycznych parametrów) – obejmującego serwery, urządzenia sieciowe i pamięci masowe, - oceny wydajności, przepustowości oraz opóźnień systemów pamięci, - predykcyjnej analityki określającej m.in. przewidywany czas awarii optyki w przełącznikach FC, - szczegółowych danych o serwerach (model, konfiguracja, wersje firmware, adresacja IP kart zarządzania),

	- parametrów serwerów, w tym: obciążenie CPU, wykorzystanie RAM, temperatury CPU i powietrza wlotowego, pobór mocy, zmiany w konfiguracji sprzętowej, z dostępem do danych historycznych i informacji o anomaliach, - parametrów pamięci masowych – opóźnienia, IOPS, przepustowość, wykorzystanie kontrolerów, pojemność całkowita i dostępna (dla całości oraz poszczególnych LUN-ów), poziom redukcji danych, status replikacji i snapshotów; dane historyczne przechowywane min. 2 lata, - parametrów przełączników sieciowych – model, adresacja IP/MAC, numery seryjne, stan komponentów (wentylatory, zasilacze), lista podłączonych hostów, wykorzystanie CPU i portów, historia parametrów oraz alerty anomali. - Aktualizacja firmware System musi umożliwiać wykonywanie aktualizacji wraz z informacją o rekomendowanych wersjach oprogramowania dla: - systemów pamięci masowych, - serwerów, - rozwiązań HCI, - przełączników FC, - deduplikatorów. - Raportowanie Muszą być dostępne raporty: - dla serwerów: nazwa hosta, model, numer seryjny, data końca kontraktu serwisowego, system operacyjny, wykorzystywany protokół komunikacyjny z pamięcią masową, średnie obciążenie CPU/RAM/IO, - dla pamięci masowych: nazwa, numer seryjny, lokalizacja, model, wersja oprogramowania, poziom zajętości wraz z redukcją danych, informacje o LUN-ach i systemach plików, status replikacji, - eksport raportów do plików CSV i PDF. Cyberbezpieczeństwo - analiza bezpieczeństwa środowiska zgodnie z najlepszymi praktykami oraz przypisanie oceny bezpieczeństwa poszczególnym urządzeniom, - powiadamianie administratora o lukach i sposobach ich zabezpieczenia, - możliwość tworzenia własnych polityk bezpieczeństwa opartych o wzorce producenta, - bieżąca analiza danych umożliwiająca wykrycie ataków ransomware, - nadawanie ról i uprawnień dedykowanych dla administratorów. Wspierane urządzenia System musi obsługiwać: - urządzenie Producenta dostarczone w ramach zamówienia, - posiadane przez Zamawiającego serwery, pamięci masowe, przełączniki sieciowe i SAN, rozwiązania HCI oraz deduplikatory Producenta. Wirtualny asystent - Funkcja wbudowanego asystenta opartego na algorytmach GenAI – z dostępem do bazy wiedzy producenta oraz możliwością analizowania danych z monitoringu infrastruktury.
--	--

	Możliwość rozbudowy - Rozszerzenie systemu o dodatkowe moduły (płatne) do monitorowania aplikacji i zarządzania incydentami IT. Funkcjonalności dodatkowe - Dedykowana aplikacja mobilna dla systemów iOS i Android.
Konsola	System powinien posiadać możliwość podłączenia konsoli zarządzającej sprzętem spełniającej poniższe warunki: • Monitorowanie stanu serwerów, w tym odczyt parametrów zdrowia, inwentarza i konfiguracji. • Konfigurowanie ustawień serwera, takich jak parametry sieci, hasła administratora i kolejność urządzeń rozruchowych. • Bezpośrednią komunikację z kontrolerem serwera za pomocą technologii bezprzewodowej. • Zdalne zarządzanie serwerami poprzez połączenie z konsolą zarządzania. • Pobieranie informacji o serwerach takich jak inwentarz, status, alerty oraz logi. • Konfigurowanie serwerów zdalnie. • Wysyłanie poleceń sterowania zasilaniem i innych poleceń. • Otrzymywanie powiadomień o alertach z systemów zarządzania. • Pobieranie informacji o gwarancji. • Uruchamianie zewnętrznych aplikacji, takich jak klienci zdalnego pulpitu. • Zabezpieczenie danych w aplikacji poprzez szyfrowanie z użyciem klucza specyficznego dla urządzenia. • Opcjonalne zabezpieczenie dostępu do aplikacji za pomocą hasła i biometrii. • Automatyczne wylogowanie w przypadku braku aktywności. • Połączenie z serwerami za pomocą technologii Bluetooth Low Energy (BLE) lub Wi-Fi. • Wyświetlanie szczegółowych informacji o serwerze oraz dzienników. • Otrzymywanie automatycznych powiadomień z konsoli zarządzania. • Przypisywanie adresów IP i modyfikowanie haseł. • Konfigurowanie atrybutów BIOS. • Wyłączanie i włączanie serwera oraz dostęp do konsoli systemowej. • Pobieranie danych z systemów zarządzania typu "jeden do wielu". • Wyświetlanie certyfikatu systemu w celu weryfikacji tożsamości przy pierwszym połączeniu.
Licencje	Oferujący zobowiązany jest do zapewnienia, dostarczenia oraz przekazania Zamawiającemu wszystkich wymaganych i niezbędnych licencji, uprawnień bądź zezwoleń, które umożliwiają pełne, prawidłowe oraz zgodne z przeznaczeniem działanie wskazanych powyżej aplikacji w całym zakresie ich funkcjonalności, zgodnym z opisem przedmiotu zamówienia. Licencje te powinny być udzielone w formie prawnej gwarantującej Zamawiającemu nieograniczoną możliwość korzystania z aplikacji zgodnie z warunkami użytkowania przewidzianymi w dokumentacji producenta, a także umożliwiać ich bieżące użytkowanie, aktualizowanie oraz integrację z innymi elementami środowiska informatycznego Zamawiającego, bez dodatkowych opłat lub utrudnień formalnych. Oferujący winien zapewnić, że dostarczone licencje pozostaną ważne i aktywne nieprzerwanie przez cały okres obowiązywania gwarancji udzielonej na dany produkt, a ich zakres czasowy oraz terytorialny będzie wystarczający do zagwarantowania możliwości korzystania z aplikacji w sposób ciągły, stabilny i bez zakłóceń. Oferujący ponosi pełną odpowiedzialność za to, aby licencje te obejmowały wszystkie moduły, rozszerzenia, komponenty oraz dodatkowe mechanizmy niezbędne do prawidłowej pracy aplikacji w praktycznym środowisku użytkownika końcowego.

	Koszt nabycia, utrzymania oraz udzielenia wymaganych licencji powinien zostać w sposób jednoznaczny, kompletny i wyraźny ujęty w wycenie przedstawionej przez Oferującego, jako integralny element całkowitej ceny oferty. Oferujący zobowiązany jest do uwzględnienia w tym koszcie wszelkich opłat licencyjnych, subskrypcyjnych, serwisowych oraz innych opłat związanych z zapewnieniem Zamawiającemu pełnych praw do korzystania z oprogramowania przez cały okres obowiązywania gwarancji. W ramach przedstawionej wyceny Oferujący powinien wziąć pod uwagę całość niezbędnych nakładów finansowych wynikających z konieczności uzyskania i utrzymania ważności licencji, tak aby Zamawiający miał zapewnioną możliwość nieprzerwanego i prawidłowego korzystania z aplikacji w pełnym zakresie ich funkcjonalności oraz bez konieczności ponoszenia dodatkowych kosztów w trakcie realizacji umowy. Wskazanie kosztów licencji w ofercie powinno być dokonane w sposób transparentny i precyzyjny, umożliwiający Zamawiającemu jednoznaczną identyfikację tej pozycji jako składowej ceny całkowitej, co pozwoli na uniknięcie ryzyka ukrytych lub nieprzewidzianych opłat po stronie Zamawiającego w okresie użytkowania oprogramowania.
Obudowa	• serwerowa do montażu w szafie RACK 19" • serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. • W obudowie powinien być zainstalowany zestaw redundantnych wentylatorów.
System zasilania i chłodzenia	System chłodzenia oferowanego rozwiązania powinien składać się z zestawu redundantnych modułów chłodzących. Moduły chłodzące powinny mieć możliwość wymiany na gorąco (hot swappable), co ułatwia ich serwisowanie i wymianę bez konieczności wyłączania serwera. Układ komponentów i konstrukcja obudowy powinny być zoptymalizowane pod kątem maksymalnego pokrycia chłodzeniem krytycznych podzespołów przy minimalnym zużyciu energii modułów chłodzących. Efektywność jednostki chłodzenia powinna być automatycznie regulowana na podstawie wielu sensorów temperatury rozmieszczonych w różnych miejscach serwera (procesor, pamięć DIMM, chipset, dyski twarde, OCP). System powinien zapewniać metody sterowania otwartą i zamkniętą pętlą, które optymalizują chłodzenie przy minimalnym poziomie hałasu i mocy wentylatorów. System musi pozwalać na konfigurację i monitorowanie parametrów chłodzenia przez wbudowane oprogramowanie zarządzające, aby mieć możliwość dostosowywania i kontrolę efektywności chłodzenia zdalnie oraz na bieżąco. Proponowane urządzenia powinny spełniać normy zgodności środowiskowej ASHRAE Class A2, obejmujące temperaturę pracy 10°C–35°C, wilgotność względną 8–80% (bez kondensacji), punkt rosy do 21°C, wysokość pracy do 3050 m n.p.m. oraz maksymalną zmienność temperatury 5°C w ciągu 20 godzin. Oferowane urządzenie powinno posiadać system zasilania, który zapewnia dynamiczną optymalizację wydajności przy jednoczesnym zachowaniu wysokiej dostępności oraz redundancji zasilania. System ten powinien umożliwiać zastosowanie zasilaczy pracujących w konfiguracjach takich jak 1+0, 2+0 (bez redundancji) oraz 1+1 (z redundancją), z funkcją automatycznego wykrywania oraz przełączania źródła zasilania w przypadku awarii. Wymagane jest, aby dostarczone zasilacze co najmniej 1100W posiadały zaawansowane technologie zmniejszania zużycia energii – w tym wysokowydajną konwersję energii,

	zaawansowane techniki zarządzania termicznego oraz wbudowane funkcje monitorowania energii o wysokiej dokładności. System powinien zapewniać stały monitoring parametrów zasilania, umożliwiając administratorowi nadzór nad zużyciem oraz szybkie reagowanie w przypadku nieprawidłowości. Dokładność pomiaru powinna wynosić 1%. Zasilacze muszą posiadać mechanizm rozpoznawania, kiedy są wyjmowane lub wkładane do serwera. System powinien automatycznie reagować na takie operacje, przełączając zasilanie na pozostałe źródło oraz generując powiadomienia dla administratora a system zarządzania powinien spowodować odpowiednią reakcję systemu chłodzenia. Funkcja ta jest kluczowa dla bezpieczeństwa i poprawnego działania redundancji oraz wyeliminowania ryzyka nieoczekiwanego wyłączenia serwera podczas wymiany modułu zasilającego.
Płyta główna	• Płyta główna z możliwością zainstalowania dwóch procesorów. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • musi być wyposażona w zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). • Numer seryjny pokazany w BIOS-ie musi być powielony na obudowie. • Musi umożliwiać utworzenie bezpiecznego profilu w oparciu o konfigurację sprzętową oraz o konfigurację wewnętrznego oprogramowania komponentów serwera. • Zintegrowany z płytą główną moduł TPM w wersji co najmniej 2.0
Procesor	• Procesor typu skalowalnego posiadający co najmniej 12 rdzeni działające co najmniej z częstotliwością 2.4GHz i dające w teście Passmark dostępnym na stronie https://www.cpubenchmark.net/ wynik nie mniejszy niż 32000 dla wersji Dual CPU
Pamięć operacyjna	• Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci taktowaną przynajmniej z częstotliwością 5600MT/s przy użyciu odpowiednich procesorów. • 128 GB pamięci RAM w modułach 32GB RDIMM przygotowanych na działanie z częstotliwością co najmniej 5600MT/s
Dyski twarde	• Serwer powinien mieć zainstalowany moduł startowanie systemu dysków M.2 skonfigurowanych w RAID1 nie zajmujących slotów na dyski. • Miejsce na co najmniej 24 dyski w rozmiarze 3.5" wymieniaalne bez wyłączania systemu. • Zainstalowane co najmniej 2 dyski minimum 1.92 Mix Use Hot-plug • Zainstalowane co najmniej 10 dysków 4TB Hot-plug
Kontroler RAID	• Serwer powinien posiadać kontroler RAID umożliwiający konfigurację RAID 0,1,5,10,50,6 posiadający co najmniej 8GB pamięci cache zabezpieczonej przed awarią prądu działający w standardzie SAS-3.
Interfejsy sieciowe/FC/SAS	• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Elementy montażowe	• Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych • Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych

Bezpieczeństwo	- 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. - 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. - Moduł 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 - Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Kontroler eksploatacji serwera	Serwer powinien być standardowo wyposażony w kontroler eksploatacji Konfigurowanie ustawień BIOS i sprzętu. Uproszczoną instalację systemów operacyjnych z wbudowanymi sterownikami, z opcją instalacji bezobsługowej dla systemów Microsoft Windows i Red Hat Enterprise Linux 7. Aktualizację oprogramowania niezależnie od systemu operacyjnego, z możliwością przywrócenia poprzedniej wersji. Ciągłą dostępność diagnostyki bez zależności od dysku twardego, z automatyczną aktualizacją oprogramowania podczas wymiany komponentów. Usunięcie danych związanych z serwerem i pamięcią masową na wybranych komponentach. Możliwe jest usunięcie informacji z BIOS. Dostarczenie informacji o bieżącej i fabrycznej konfiguracji systemu. Udostępnianie logów sprzętowych w celu rozwiązywania problemów. Zdalne zarządzanie cyklem życia serwera co najmniej za pomocą interfejsu WS-Man Konfigurację ustawień sieci dla wbudowanej karty NIC, w tym ustawienia VLAN. Wykonywanie diagnostyki pamięci, urządzeń we/wy, procesora i dysków fizycznych. Aktualizację komponentów systemu za pomocą repozytoriów lub pojedynczych pakietów DUP. Powrót do poprzedniej wersji oprogramowania układowego. Umożliwia zabezpieczenie konfiguracji systemu - "System Configuration Lockdown mode" Automatyczną aktualizację oprogramowania i konfiguracji wymienionych części. Trwałe usunięcie danych przed ponownym wykorzystaniem lub wycofaniem systemu. Obsługę różnych metod aktualizacji, za pomocą różnych źródeł, takich jak FTP, udziały sieciowe (CIFS, NFS, HTTP, HTTPS) lub lokalne napędy USB/DVD
Karta Zarządzania	- Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą: - zdalny dostęp do graficznego interfejsu Web karty zarządzającej - szyfrowane połączenie (TLS) oraz autentykację 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 poprzez złącze RS-232. ○ - możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy. ○ - 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 zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych • - Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram.
Normy	Proponowane urządzenie powinno spełniać normy zgodności środowiskowej ASHRAE Class A2, obejmujące temperaturę pracy 10°C–35°C, wilgotność względną 8–80% (bez kondensacji), punkt rosy do 21°C, wysokość pracy do 3050 m n.p.m. oraz maksymalną zmienność temperatury 5°C w ciągu 20 godzin. System powinien być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 Produkt złożony lub zbudowane urządzenie, które jest składane z elementów posiadających indywidualnie deklarację CE, nie posiada automatycznie całościowej deklaracji zgodności CE dla tego zbudowanego produktu. W przypadku składania lub montażu takich komponentów w nowy, kompletny produkt, wymagane jest sporządzenie odrębnej, całościowej deklaracji zgodności CE dla finalnego wyrobu. Oznacza to, że firma dokonująca złożenia produktu z elementów musi przeprowadzić odpowiednią ocenę zgodności całego urządzenia, uwzględniając integralność, bezpieczeństwo i inne obowiązujące normy oraz wymogi prawne. Brak całościowej deklaracji zgodności CE dla złożonego produktu może skutkować konsekwencjami prawnymi, ograniczeniami w wprowadzeniu produktu do obrotu oraz ryzykiem odpowiedzialności za ewentualne zagrożenia wynikające z użytkowania urządzenia. Podsumowując, posiadanie deklaracji CE dla pojedynczych elementów nie zwalnia z obowiązku uzyskania i wystawienia całościowej deklaracji zgodności CE dla całego, złożonego produktu, co jest warunkiem legalnej sprzedaży i użytkowania tego produktu na rynku Unii Europejskiej i dlatego też oferowane urządzenie jako całość musi posiadać deklaracja CE.
Certyfikaty	Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu

	jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver do użycia na terenie Polski zarejestrowany w Polsce według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu.
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	- Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat. - Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. - Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. - Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. - Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. - Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. - Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. - Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. - Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: - Możliwości utworzenia zgłoszenia serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. - Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. - Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. - Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. - Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaze dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.

	Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.
Producenci wysokiego ryzyka	Zamawiający nie dopuszcza ofert producentów z krajów wysokiego ryzyka, gdyż istnieje, możliwość że jej łańcuch dostaw zostanie zablokowany co uniemożliwi jej świadczenie usług wsparcia. firma, której rozwiązania są oferowane, nie może być na liście wysokiego ryzyka, w którymś z państw UE, US, UK, CA, JPN, AU Ze względu na wymogi bezpieczeństwa, Wykluczenie firm, które są: • producentami/dostawcami produktów wysokiego ryzyka; • objęte zakazem eksportu (nie będą mogli świadczyć usług wsparcia, jeśli nie dostaną komponentów produkowanych w krajach demokratycznych); • powiązane bezpośrednio (w tym osobowo) z podmiotami objętymi sankcjami Listy wysokiego ryzyka: USA: https://www.congress.gov/bill/115th-congress/house-bill/5515/text USA: https://www.bis.doc.gov/index.php/documents/consolidated-entity-list/915-consolidated-list-csv/file USA: https://data.trade.gov/downloadable_consolidated_screening_list/v1/consolidated.csv EU: https://data.europa.eu/data/datasets/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions?locale=en UK: https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets Unia Europejska (ogół) (29 stycznia 2020) – definiuje „high-risk vendors” i środki strategiczne dla krajów członkowskich Komisja UE – ogłoszenie 2020 https://ec.europa.eu/commission/presscorner/detail/en/statement_23_3312
Portal wsparcia produktu	W ramach wsparcia technicznego wymagana jest usługa polegająca na przygotowaniu i dostarczeniu spersonalizowanego panelu w chmurze Usługa powinna pozwalać na identyfikowanie priorytetów i potencjalnych zagrożeń technicznych sprzętu co pomoże w podejmowanie właściwych działań. Usługa powinna spełniać następujące założenia/funkcje: - Proaktywne zarządzanie priorytetami usług serwisowych w tym graficzną reprezentację poziomu zagrożeń. - Możliwość personalizacji widoku przez członków zespołu do zarządzanych przez nich lokalizacji i zasobów. - Dostęp do szczegółów dotyczących sprzętu i oprogramowania, w tym incydentów krytycznych, wsparcia technicznego, eskalacji, konserwacji na miejscu, poziomów kodu, poradników bezpieczeństwa i technicznych, zakresu wsparcia, wymiany części, łączności urządzeń i bram. - Dostęp do danych historycznych i analiz na potrzeby planowania IT

Oprogramowanie \\ system operacyjny	Windows Server 2025 Datacenter -16 Core/ Licencja Wieczysta/ EDU na tenancie podanym przez zamawiającego.
--	---