ZP.271.2.1.2026 **Dostawa sprzętu informatycznego i oprogramowania wraz z wdrożeniem w ramach projektu grantowego „Cyberbezpieczny samorząd”**

Załącznik nr 8 do SWZ

Szczegółowy opis przedmiotu zamówienia

CZĘŚĆ I

System zasilania awaryjnego dla urządzeń przetwarzających dane

a) Zasilacz awaryjny – 1 szt.

Nazwa komponentu		Wymagane minimalne parametry techniczne
Moc		40 kVA/40kW
Typ		On-Line / podwójna konwersja
Typ zabudowy		wolnostojący TOWER
Konstrukcja		Modułowy, falownik, prostownik, bypass i ładowarka w zestawie;
Wejście - zasilanie	Liczba faz	3
	Napięcie znamionowe	380 / 400 / 415 V
	Częstotliwość znamionowa	50 / 60 Hz (autodetekcja)
	Współczynnik mocy (PF)	≥ 0,99
Układ obejścia (bypass)	Typ	Wewnętrzny elektroniczny
	Napięcie znamionowe	380 / 400 / 415 V
	Częstotliwość znamionowa	50 / 60 Hz
	Wbudowany rozłącznik toru obejścia	
Akumulatory	Dopuszczalne technologie akumulatorów	VRLA / AGM / NiCd / Li
	Układ połączeń	pakiety akumulatorowe ze stykami kontrolnymi
	Napięcie nominalne	± 480 V DC (VRLA/AGM)
	Ilość akumulatorów wewnętrznych	80 szt. (VRLA/AGM)
	Pojemność akumulatorów wewnętrznych	10 Ah (VRLA/AGM)
	Pojemność akumulatorów zewnętrznych	konfigurowalna
	Montaż akumulatorów	wewnątrz UPS
	Prąd ładowania nominalny	40 A
	Możliwość podłączenia zewnętrznych akumulatorów	
	Praca z akumulatorami wewnętrzne + zewnętrzne	
	Wbudowany rozłącznik toru akumulatorów	
Wyjście	Liczba faz	3
	Napięcie wyjściowe	380 / 400 / 415 V (konfigurowalne)
	Częstotliwość przy pracy z	50 / 60 Hz

	sieci	
	Częstotliwość przy pracy z akumulatorów	50 / 60 Hz
	Przebieg napięcia	fala sinusoidalna
	Współczynnik mocy (PF)	1
	Współczynnik szczytu (CF)	3:1
	Zdolność przeciążeniowa	102 ÷ 110 % do 60 min 111 ÷ 125 % do 10 min
System	Sprawność	95%
	Czas przełączenia	0 ms
	Funkcje rozruchu	Zimny i miękki start;
	Interfejs użytkownika	Kolorowy ekran dotykowy o przekątnej 5 cali' Diagram stanu pracy z sygnalizacją stanu bypassu zewnętrz-nego Przypomnienia dla: - przeglądu okresowego - wymiany akumulatorów - wymiany kondensatorów - wymiany wentylatorów
	Zabezpieczenia	Autodiagnostyk systemu i interfejsu użytkownika Powłoka ochronna; Zwarciowe Przeciążeniowe Termiczne;
Komunikacja	Złącza	karty rozszerzeń: SNMP RS485 / MODBUS styki bezpotencjałowe
	Wspierane protokoły komunikacyjne	http, HTTPS, FTP; FTPS; SNMP, Modbus, NTP; SSH; SMTP; Sy-slog, RADIUS; LDAP; 802.1X;
	Bezpieczeństwo	Kontrola dostępu do ustawień UPSa Ustawienie haseł; Stopień ochrony - IP 20 z filtrem przeciwpyłowym w przed-niej osłonie
Instalacja i uruchomienie		1. Montaż bez zakłócania pracy Urzędu, 2. Montaż zewnętrznego bypassa, 3. Podłączenie UPS wraz I modułu bateryjnego do instalacji zamawiającego 4. Montaż i konfiguracja karty SNNP; 5. Uruchomienie i przetestowanie systemu; 6. Przeszkolenie użytkowników; 7. Pomiary elektryczne po instalacji;
Wymagania dodatkowe		Instalacja i konfiguracja oraz integracja z siecią elektryczna zamawiającego

	Dostęp serwisowy System kontroli akumulatorów Wbudowany rozłącznik toru wyjściowego Złącze EPO; Aktywne odprowadzanie ciepła; Filtr przeciwzakłóceniowy RFI i EMI Technologia eliminująca pojedyncze punkty krytyczne; Możliwość monitorowania stanu UPS oraz sterowania urządzeniami przez styki bezpotencjałowe Zasilacz musi być wyprodukowany zgodnie z normą ISO 9001
Warunki gwarancji	24 miesiące na elektronikę; 12 miesięcy na baterie; Serwis musi być świadczony w trybie on site (w miejscu instalacji zestawu);

b) Agregat prądotwórczy – 1 szt.

Nazwa parametru	Wymagane minimalne parametry techniczne
Obudowa	1. Stalowa, pomalowana proszkowo; 2. Oporna na niekorzystne warunki atomosferyczne oraz wandalizm 3. Boczne drzwi mocowane na zawiasach ze stali nierdzewnej z klamką; 4. Zamykane drzwi zabezpieczające panel sterowania; 5. Boczna czerpnia powietrza zabezpieczona i wyciszona; 6. Górna zabezpieczona wyrzutnia powietrza. 7. Odłączalny uchwyt transportowy z możliwością odłączenia. 8. Tłumik wyciszającywewnątrz obudowy
Panel sterowania	1. Z możliwością programowania podstawowych parametrów pracy. 2. Zabezpieczony zamykanymi drzwiami z wizjerem; 3. Wbudowany port komunikacyjny;
Sterowanie	1. Tryby pracy: ręczny start, automatyczny start, automatyczny test; 2. Przyciski wymuszenia zasilania z agregatu lub z sieci 3. Przyciski: start/stop, reset błędu; 4. Wyłącznik awaryjny; 5. Możliwość zdalnego startu. 6. Wyłącznik zasilania; 7. Automatyczny prostownik akumulatora 8. Możliwość ustawienia hasła bezpieczeństwa
Współczynnik mocy	φ 0.8;
Liczba faz	3;
Moc maksymalna	70 kVA/60 kW
Moc znamionowa	70 kVA/55 kW;
Emisja spalin	Non Emission Certified
Chłodzenie silnika	4000 cm^3

Zasilanie	Turbodoładowany z intercoolerem	
Regulator obrotów	Elektroniczny	
Pojemność układu smarowania	8 litrów;	
Paliwo	Olej napędowy (diesel);	
Zużycie paliwa	Maksymalnie 220 g/kWh; Przy 75% PRP – maksymalnie 14 l/h Przy 100% PRP – maksymalnie 20 l/h	
System rozruchu	elektryczny	
Silnik	Wysokoprężny, zapewniający stabilizację częstotliwości i diagnostykę oraz posiadający wyłącznik;	
Prądnica	Napięcie	400V;
	Typ	Bezszczotkowa
	Bieguny	4 szt.
	Typ AVR	Cyfrowy DSR;
	Tolerancja napięcia	Maksymalnie 1%;
	Sprawność	90%
	Klasa IP / izolacji	20/H
System wzbudzenia	Alternator poskokiem 2/3; Brak krotności trzeciej harmonicznej (3, 9, 15, itd.) napięcia wyjściowego. Minimalizacja indukowania się nadmiernych prądów w obwodzie neutralnym. Uzwojenie dodatkowe w stojanie zasilającym regulator napięcia musi umożliwiać przejęcie 300% obciążenia znamionowego przez co najmniej 20 sekund. Niezawodny rozruch silnika elektrycznego; Uzwojenia musza być zaimpregnowane żywicą epoksydową; Alternator musi być wykonany zgodnie z normami CEI 2-3 i IEC 34-1;	
Zbiornik paliwa	Pojemność – 120 litrów; Wykonany z trwałego plastiku; Wlew, wentylacja, czujnik poziomu paliwa; Rurka spustowa oleju;	
Gwarancja	12 miesięcy w miejscu instalacji urządzenia; Fabrycznie nowe, bez śladu użytkowania; Musi pochodzić z autoryzowanego kanału sprzedaży na rynek polski; Musi posiadać serwis i wparcie producenta.	
Wymagania dodatkowe	Zapewnienie poprawnej konfiguracji oraz automatycznego włączenia w przypadku braku zasilania (ATS/SZR), Instalacja i konfiguracja oraz integracja z siecią elektryczną zamawiającego; Szkolenie z obsługi przy dostawie; Podstawa ze spawanych profili stalowych wyposażona w amortyzatory drgań oraz spawane nogi;	

CZĘŚĆ II

I. Serwer do klastra HA – 1 szt. – Typ I

1. Praca obydwu serwerów w klastrze musi odbywać się zgodnie z polityką licencyjną producenta oferowanego systemu operacyjnego oraz musi uwzględniać fakt, że na klastrze będą pracowały 2 maszyny wirtualne z zainstalowanym systemem operacyjnym opisanym w tabeli poniżej;
2. Obok klastra wirtualizacyjnego, na obydwu serwerach musi zostać zainstalowane opisane poniżej oprogramowanie bazodanowe (bezpośrednio na hostach fizycznych);
3. Klaster musi umożliwiać przejęcie przez serwer zapasowy, obciążenia serwera podstawowego, w przypadku braku jego dostępności np. w wyniku awarii;

Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	Obudowa Rack o wysokości maksymalnie 1U z możliwością instalacji 8 dysków 2.5" NVMe;
Płyta główna	Obsługa procesorów 32 rdzeniowych. Szesnaście slotów przeznaczonych do instalacji pamięci. Obsługa do 1 TB pamięci RAM ECC DDR5 6400 MT/s;
Procesor	Zainstalowany procesor maksymalnie 32-rdzeniowy osiągający wynik 74 000 w teście PassMark CPU Mark – **załączyć do oferty wydruk ze strony** www.cpubenchmark.net lub www.passmark.com.
Pamięć RAM	256 GB DDR5 RDIMM 6400MT/s, moduły dwubankowe;
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający ○ Możliwość konfiguracji poziomów RAID: 0, 1, 10; ○ Wsparcie dla dysków SAS, SATA i NVMe; ○ Wsparcie dla PCIe gen. 4;
Dyski twarde	Zainstalowane 4 x 960 GB NVMe U2 do intensywnego odczytu
Gniazda PCI	Pięć slotów PCIe
Interfejsy sieciowe	2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Wbudowane porty	• 4 porty USB w tym min: ○ 2 port USB 3.1 z tyłu obudowy, ○ 1 port USB typu C z przodu obudowy • 1 port VGA • 1 x RJ45
Wentylatory	Redundantne, Hot-Plug
Zasilacz	Redundantny, Hot-Plug 1500W każdy, klasy Titanium;
Elementy montażowe	Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych
Bezpieczeństwo	1. Firmware podpisany kryptograficznie; 2. Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.

	3. Sprzętowe szyfrowanie danych w stanie spoczynku, przechowywanych na dyskach na wypadek ich kradzieży; 4. Klucze szyfrujące muszą być przechowywane oddzielnie od danych; 5. Bezpieczny rozruch UEFI poprzez weryfikację podpisu cyfrowego komponentów rozruchowych przed załadowaniem systemu operacyjnego; 6. Wbudowany czujnik otwarcia obudowy; 7. Moduł TPM 2.0 8. Mechanizm umożliwiający weryfikację integralności firmware gwarantujący, że podczas rozruchu serwera ładowany jest wyłącznie autentyczny kod; 9. Możliwość usunięcia danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem; 10. Tryb blokady konfiguracji i aktualizacji oprogramowania sprzętowego. Po zablokowaniu systemu wszelkie próby zmiany konfiguracji muszą być blokowane. W przypadku próby zmiany krytycznych ustawień systemowych wyświetlany musi być komunikat o błędzie; 11. Automatyczne odzyskiwanie głównego obrazu BIOS/obrazu odzyskiwania
Karta zdalnego zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego karta zdalnego zarządzania, posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: 1. Zdalny dostęp do interfejsu graficznego serwera z dowolnego miejsca z przeglądarką internetową (wirtualna konsola**)** 2. Możliwość podłączenia obrazów ISO lub dysków USB w celu instalacji oprogramowania lub diagnostyki. 3. Śledzenie parametrów pracy serwera i generowanie powiadomień w przypadku wykrycia problemów. 4. Optymalizacja zużycia energii przez serwer. 5. Możliwość zdalnego uruchamiania i wyłączania serwera. 6. Uwierzytelnianie, autoryzacja i szyfrowanie danych; 7. zarządzanie serwerem za pomocą interfejsu graficznego przez przeglądarkę lub interfejsu wiersza poleceń (CLI); 8. Skanowanie BIOS-u musi weryfikować integralność i autentyczność obrazu BIOS-u;. Pomyślny wynik skanowania musi być rejestrowany w dzienniku kontrolera cyklu życia 9. Ochrona przed lukami w oprogramowaniu, próbami włamań i złośliwym oprogramowaniem. Proces systemowy, nie może uzyskać dostępu do plików ani sprzętu, które są poza jego zakresem; 10. Wsparcie dla SSH; 11. Szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika 12. Wirtualna konsola z dostępem do myszy, klawiatury 13. Wsparcie dla IPv6 14. Wsparcie dla SNMP; IPMI2.0, VLAN tagging, 15. Integracja z Active Directory 16. Wsparcie dla LLDP 17. Wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej

	18. Możliwość podłączenia lokalnego poprzez złącze RS-232. 19. Automatyczne update firmware dla wszystkich komponentów serwera 20. Możliwość przywrócenia poprzednich wersji firmware 21. Możliwość eksportu/importu konfiguracji karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID do pliku XML lub JSON 22. Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych 23. Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram. 24. Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera 25. Serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej;
System operacyjny	Posiadający następujące, wbudowane funkcjonalności: 1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny system operacyjny. 3. 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. 4. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 6. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 7. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 8. 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). 9. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 10. Licencja musi uprawniać do zainstalowania systemu w środowisku fizycznym oraz na dwóch maszynach (instancjach) wirtualnych; 11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.

	12. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET 13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18. 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), 19. 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.. 20. Oferowana licencja musi umożliwiać, zgodną z polityką licencyjną producenta system operacyjnego, pracę na serwerze wyposażonym w trzydzieści dwa rdzenie procesorowe; 21. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 22. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 23. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 24. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 25. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 26. 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 8.1. 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: • 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) 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) Wsparcie dla algorytmów Suite B (RFC 4869), l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputera m) 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: • 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) 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. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 30. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 31. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. Zorganizowany system szkoleń i materiały edukacyjne w języku polski	
Oprogramowanie bazodanowe	Silnik bazy danych	Przechowywanie, przetwarzanie i zabezpieczanie danych, replikacji, pełnotekstowego wyszukiwania, narzędzi do zarządzania danymi relacyjnymi i XML, integracja z analityką baz danych w celu uzyskania dostępu do heterogenicznych źródeł danych, a także usługi Machine Learning umożliwiające uruchamianie skryptów z danymi relacyjnymi.
	Usługi analityczne	Muszą obejmować narzędzia do tworzenia i zarządzania aplikacjami do przetwarzania analitycznego online (OLAP) i eksploracji danych.
	Usługi raportowania	Muszą obejmować komponenty serwera i klienta do tworzenia, zarządzania i wdrażania raportów tabelarycznych, macierzowych, graficznych i w formie swobodnej. Muszą stanowić rozszerzalną platformę do tworzenia aplikacji raportujących;
	Usługi integracyjne	Zestaw graficznych narzędzi i programowalnych obiektów do przenoszenia, kopiowania i przekształcania danych. Muszą obejmować moduł jakości danych;
	Usługi danych głównych	Rozwiązanie do zarządzania danymi głównymi. Możliwość konfiguracji do zarządzania dowolną domeną (produkty, klienci, konta); Musi zawierać hierarchię, szczegółowe zabezpieczenia, transakcje, wersjonowanie danych i reguły biznesowe, a także dodatek do arkusza kalkulacyjnego do zarządzania danymi.
	Usługi uczenia maszynowego w bazie danych	Obsługa rozproszonych, skalowalnych rozwiązań uczenia maszynowego przy użyciu źródeł danych; Obsługa języków programowania R i Python.
	Wirtualizacja danych	Obsługa zapytań dotyczących różnych typów danych w różnych typach źródeł danych z poziomu programu;
	Usługi połączone z platformą chmurową	Musi poszerzać usługi i funkcje platformy chmurowej producenta oprogramowania takie jak: zasady dostępu i rozliczanie według zużyci;.
	Licencja	Wieczysta, niewygasająca. Zamawiający nie może być zobowiązany do ponoszenia jakichkolwiek kosztów w celu zachowania prawa do korzystania z tej

		licencji w przyszłości; Musi umożliwiać, zgodnie z polityką licencyjną producenta, instalację na dwóch serwerach fizycznych oraz pracę/dostęp dla trzydziestu użytkowników w sieci zamawiającego;
	Rozmiar danych zoptymalizowany pod kątem pamięci na bazę danych	16 GB;
	Maksymalny rozmiar relacyjnej bazy danych	524 TB;
	Wysoka dostępność	Kopiowanie bazy danych Serwery failover do odzyskiwania po awarii w usłudze chmurowej; Kompresja kopii zapasowej Migawka bazy danych Zawsze włączone instancje klastra failover dla 2 węzłów Obsługa podstawowych grup dostępności, z których każda musi obsługiwać 2 repliki z jedną bazę danych; Szyfrowana kopia zapasowa Tworzenie kopii zapasowych i przywracanie do pamięci masowej obiektów zgodnej z S3; Kopia zapasowa migawki Serwery awaryjne do odzyskiwania po awarii Serwery failover zapewniające wysoką dostępność
	Skalowalność i wydajność	Magazyn kolumn Duże obiekty binarne w klastrowanych indeksach magazynu kolumn OLTP w pamięci Hybrydowy bufor puli Obsługa pamięci trwałej Partycjonowanie tabel i indeksów Kompresja danych Paralelizm tabeli partycjonowanej Wiele kontenerów strumieni plików Rozszerzenie puli buforowej Równoległe skanowanie puli buforów Odroczona kompilacja zmiennej tabeli Skalarne wstawianie UDF Przeplatane wykonywanie funkcji o wartościach tabelarycznych zawierających wiele instrukcji; Zintegrowane przyspieszanie i odciążanie;
	Bezpieczeństwo	Audyt bazy danych Bazy danych zawsze szyfrowane z bezpiecznymi enklawami Dynamiczne maskowanie danych Szyfrowanie kopii zapasowych

		Rozszerzalne zarządzanie kluczami Bezpieczeństwo na poziomie wiersza bazy danych; Audyt serwera Przeźroczyste szyfrowanie danych (TDE)
	Replikacja	Replikacja scalająca Replikacja migawek Śledzenie zmian w programie bazy danych; Replikacja transakcyjna, w tym również do platformy chmurowej; Subskrypcja z możliwością aktualizacji replikacji transakcyjnej
	Zarządzanie	Obiekty zarządzania Ocena podatności Menedżer konfiguracji Profiler; Agent serwera Dostrajanie bazy danych Dedykowane połączenie administracyjne Obsługa skryptów PowerShell Obsługa operacji komponentów aplikacji warstwy danych — wyodrębnianie, wdrażanie, uaktualnianie, usuwanie Automatyzacja zasad - sprawdzanie harmonogramu i zmiana Standardowe raporty wydajności Przewodniki po planach i zamrażanie planów dla przewodników po planach Bezpośrednie zapytanie do widoków indeksowanych; Automatyczna konserwacja widoków indeksowanych Rozszerzenie puli buforowej Główna instancja dla klastra dużych danych Certyfikacja zgodności
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 - **załączyć do oferty certyfikaty dla producenta;** • Oferowane urządzenie musi pochodzić z oficjalnego kanału dystrybucji producenta na rynek polski – **załączyć do oferty oświadczenie producenta;** • Aktywny certyfikat EPEAT dla Polski, co najmniej na poziomie SILVER, wydany nie wcześniej niż w roku 2024 – załączyć do oferty wydruk ze strony internetowej www.epeat.net – **załączyć do oferty;**	
Gwarancja	• 36 miesięcy NBD on site producenta serwera; • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania, w tym także oprogramowania. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/portal) 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.	

	• Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Uszkodzone dyski pozostają własnością zamawiającego;

II. Przełączniki sieciowe – 9 szt.

a) Przełącznik Typ I – 8 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Porty	48 x Gb RJ45 PoE z czego 40 portów o mocy 32W i 8 portów o mocy 64W; 4 x 10 Gb SFP+; 1 x port konsolowy RJ45;
Warstwa 3	Routing statyczny między sieciami VLAN; Funkcjonalność serwera i przełącznika DHCP
Warstwa 2	LACP, STP & RSTP, QoS, IGMP, Listy kontroli dostępu ACL oparte na adresach MAC; Izolacja urządzeń; Flow & Storm control; Ograniczanie szybkości transmisji wielokierunkowej i rozgłoszeniowej Blokowanie adresów MAC; Ograniczenie funkcji portu na podstawie adresu MAC Izolowanie i mirroring portów; LLDP-MED.; Dedykowany VLAN dla połączeń głosowych;
Transfer danych	130 Gbps
Wydajność przełączania	176 Gbps;
Przepustowość nieblokująca	88 Gbps;
PoE	8 portów o mocy 60W na port; Łączna dostępna moc – 600W; Automatyczne wykrywanie standard PoE;
Raportowanie	Konfigurowalne raportowanie i analizy, umożliwiające zarządzanie użytkownikami; Wyszukiwanie i sortowanie zwiększające efektywność zarządzania siecią.
Chłodzenie	Wentylatory z czujnikami temperatury oraz wbudowanym systemem zarządzania mocą;;
Zasilacz	650W, redundantny;
Zużycie prądu	Maksymalnie 60W bez PoE i 650W z PoE;
Zgodnośc z normami	ETSI300-019-1.4, NDAA;
VLAN	Obsługa 100 sieci;
Tabela adresów MAC	16 000;;
Tabele warstwy 3	ARP – 4000; IPv4 – 1000;
Bufor pakietów	4 MB;

Listy dostępu	IPv4 – 128; MAC – 128;
Warunki gwarancji	36 miesięcy;
Wymagania dodatkowe	Możliwość montażu w szafie rack; Wyświetlacz dotykowy do monitorowania kondycji przełącznika i rozwiązywania problemów;

b) Przełącznik Typ II – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Porty	28 x 10 Gb SFP+; 4 x 25Gb SFP28
Warstwa 3	Routing statyczny między sieciami VLAN; Funkcjonalność serwera i przełącznika DHCP
Zarządzanie	1. Konfigurowanie i monitorowanie wszystkich funkcji przełącznika za pośrednictwem GUI z dowolnego miejsca z dostępem do internetu; 2. Interfejst zarządzający - Ethernet
Zasilanie	100W, redundantne;
Transfer danych	560 Gbps
Wydajność przełączania	760 Gbps;
Przepustowość nieblokująca	380 Gbps;
VLAN	Obsługa 100 sieci;
Tabela adresów MAC	32 000;;
Tabele warstwy 3	ARP – 16 000; IPv4 – 16 000;
Bufor pakietów	4 MB;
Listy dostępu	IPv4 – 128; MAC – 128;
Warstwa 2	LACP, STP & RSTP, QoS, IGMP, Listy kontroli dostępu ACL oparte na adresach MAC; Izolacja urządzeń; Flow & Storm control; Ograniczanie szybkości transmisji wielokierunkowej i rozgłoszeniowej Blokowanie adresów MAC; Ograniczenie funkcji portu na podstawie adresu MAC Izolowanie i mirroring portów; LLDP-MED; Obsługa ramek Jumbo Dedykowany VLAN dla połączeń głosowych; Ochrona przed pętlami
Zużycie prądu	Maksymalnie 100W;
Warunki gwarancji	36 miesięcy;
Wymagania dodatkowe	Możliwość montażu w szafie rack; Wyświetlacz dotykowy do monitorowania kondycji przełącznika i rozwiązywania problemów;

	Zabezpieczenie ESD;

c) Kontroler

Nazwa komponentu	Wymagane minimalne parametry techniczne
Procesor	Osiągający wynik 2400 w teście PassMark CPU Mark – **załączyć do oferty wydruk ze strony www.cpubenchmark.net lub www.passmark.com.**
Pamięć RAM	2 GB;
Pamięć flash	32 GB;
Porty	2 x Ethernet
Interfejs fo konfiguracji	Bluetooth, przeglądarka siec web;
Zasilanie	PoE;
Zużycie energii	Maksymalnie 5W;
Wymagane funkcje	1. Monitorowanie i zarządzanie zaoferowanymi przełącznikami sieciowymi; 2. Samodzielny serwer aplikacji; 3. Musi umożliwiać konfigurację chmury hybrydowej oraz SSO; 4. Panel sterowania umożliwiający dodawanie i udostępnianie przełączników sieciowych; 5. GUI; 6. Możliwość zarzadzania urządzeniami w różnych lokalizacjach; 7. Konfigurowalne raporty i analizy; 8. Tworzenie wielu grup LAN i WLAN; 9. Mapowanie sieci; 10. Zarządzanie ruchem; 11. Funkcje wifi: - monitorowanie częstotliwości radiowych i mapowanie urządzeń - analiza wydajności poszczególnych częstotliwości radiowych; - sterowanie pasmem; - obsługa hotspot; 12. Obsługa bram i przełączników, w tym co najmniej:; - konfiguracja WAN, LAN i VLAN - różne tryby pracy, w tym co najmniej: przełączanie, dublowanie lub agregacja dla każdego portu; - możliwość ustawienia opcji różnych PoE dla każdego portu w zależności od podłączonego do niego urządzenia; 13. Obsługa ranek jumbo i kontroli przepływu; 14. Monitorowanie i analiza wydajności każdego portu; 15. Wizualna prezentacja stanu sieci; 16. Aplikacja mobilna producenta kontrolera; 17. Informacje o opóźnieniach i przepustowości każdego zarządzanego urządzenia; 18. Tworzenie map, w tym niestandardowych obrazów lokalizacji oraz korzystanie z aplikacji zewnętrznych udostępniających mapy; 19. Informacje o okolicznych sieciach bezprzewodowych, statystykach

	klientów; 20. Prezentacja zdarzeń i aktywności w sieci, w tym błędów i ostrzeżeń; 21. Przeglądanie topologii i konfiguracji sieci, statystyk w czasie rzeczywistym oraz metryk debugowania; 22. Inspekcja pakietów zawierająca najnowsze sygnatury identyfikacyjne aplikacji. Sygnatury muszą pozwalać śledzić, które aplikacje i adresy IP wykorzystują najwięcej przepustowości; 23. Ustawienia sieciowe i storm control dla każdego portu 24. Konfiguracja STP; 25. Debugowanie dla interfejsu wiersza poleceń 26. Możliwość przeglądania informacji o stanie każdego portu, w tym co najmniej: a) prędkość połączenia i tryb dupleksu b) przepływność danych TX/RX c) ustawienia sieci/VLAN 27. Scentralizowane zarządzanie konfiguracją, w tym jej klonowanie; 28. Auto-MDIX; 29. Uwierzytelnianie 802.1X (RADIUS) i dynamiczna sieć VLAN
Warunki gwarancji	36 miesięcy; Live chat z dostępem do inżyniera wsparcia technicznego w trybie 24/7;
Wymagania dodatkowe	Możliwość montażu w szafie rack;

III. System SIEM

a) **Cel wdrożenia:**

1. Wzrost poziomu bezpieczeństwa IT w organizacji
2. Monitorowanie i analiza zdarzeń w systemach IT,
3. Szybkie wykrywanie incydentów bezpieczeństwa
4. Spełnienie wymagań regulacyjnych dotyczących bezpieczeństwa danych,
5. Optymalizacja reakcji na zagrożenia i automatyzacja odpowiedzi na incydenty

b) **Wymagania funkcjonalne wobec oprogramowania:**

1. System musi zapewniać monitoring bezpieczeństwa i ochronę zasobów IT;
2. System musi chronić zasoby cyfrowe i wzmacniać cyberbezpieczeństwo w urzędzie;
3. Monitorowanie ustawień konfiguracji aplikacji dla zapewnienia ich zgodności z politykami bezpieczeństwa, standardami i/lub wytycznymi dotyczącymi zabezpieczeń;
4. Okresowe skanowanie w celu wykrycia błędnych konfiguracji lub luk w zabezpieczeniach punktów końcowych, które mogą zostać wykorzystane przez atakujących.
5. Możliwość dostosowania kontroli konfiguracji do potrzeb urzędu;

6. Alerty bezpieczeństwa zawierające zalecenia dotyczące lepszej konfiguracji, odniesienia i mapowanie zgodnie z przepisami;
7. Ocena konfiguracji zabezpieczeń pod kątem zgodności z najlepszymi praktykami i standardami bezpieczeństwa;
8. Skanowanie monitorowanych punktów końcowych za pomocą testów porównawczych;
9. Instrukcje dotyczące usuwania luk w konfiguracji, wzmacniania zabezpieczeń systemu i ograniczania powierzchni ataku;
10. Kontrole konfiguracji na punktach końcowych i obciążeniach chmurowych;
11. Kontrole dla różnych systemów operacyjnych hostowanych lokalnie lub w chmurze;
12. Możliwość tworzenia niestandardowych kontroli konfiguracji;
13. Regularne sprawdzanie monitorowanych punkty końcowych w celu zapewnienia zgodności z przepisami I wewnętrznymi standardami;
14. Przechowywanie logów, indeksowanie i wyszukiwanie w celu badania zagrożeń, które mogły ominąć wstępne kontrole bezpieczeństwa;
15. Reguły wykrywania zagrożeń muszą być mapowane na strukturę MITRE ATT&CK;
16. Badanie i odwoływanie się do taktyk, technik i procedur powszechnie stosowanych przez atakujących;
17. Integracja z zewnętrznymi kanałami i platformami analizy zagrożeń;
18. Agenci musza pobierać dane inwentaryzacyjne oprogramowania i przesyłać je do serwera;
19. Dane muszą być korelowane z aktualizowanymi bazami danych;
20. Identyfikacja znanego i podatnego oprogramowania;
21. Automatyczne wykrywanie luk w zabezpieczeniach;
22. Analiza danych z logów musi obejmować przeglądanie logów generowanych przez urządzenia sieciowe, punkty końcowe i aplikacje;
23. Gromadzenie, analiza i przechowywanie logów z infrastruktury w czasie rzeczywistym;
24. Eliminacja silosów bezpieczeństwa;
25. Integracja z platformami analizy zagrożeń, systemami zapobiegania włamaniom, platformami zgłoszeń;
26. Pełna widoczność całej infrastruktury IT zamawiającego;
27. Musi wykrywać złośliwe działania i oznaki naruszenia bezpieczeństwa, które występują na punktach końcowych w wyniku infekcji złośliwym oprogramowaniem lub cyberatak;
28. Gotowy zestaw reguł takich jak ocena konfiguracji zabezpieczeń, rootcheck i monitorowanie integralności plików;
29. Możliwość skonfigurowanie i dostosowania tych funkcji do wymagań zamawiającego;
30. System musi wykrywać co najmniej: ransomware, rootkity, spyware, adware, trojany, wirusy i robaki;
31. Możliwość dodawania niestandardowych reguł I dekoderów wykrywających nowe sygnatury I zachowania złośliwego oprogramowania;
32. Badanie monitorowane punkty końcowe pod kątem niespójności, takich jak ukryte porty, nietypowe pliki i uprawnienia, ukryte procesy oraz awarie oprogramowania;
33. Zbieranie logów z wykorzystaniem agentów i bez agentów;
34. Korelowanie zdarzeń z wielu źródeł logów w celu wykrywania złośliwego oprogramowania i szkodliwego działania;
35. Wizualizacja i analiza skorelowanych zdarzeń;

36. Monitorowanie i powiadamianie o zmianach w krytycznych plikach i katalogach w czasie rzeczywistym;
37. Wykrywanie naruszenia bezpieczeństwa i manipulacji systemem;
38. Wbudowany load balancer umożliwiający dystrybucję obciążeń na wiele węzłów;
39. Możliwość tworzenia inwentarzy punktów końcowych i aplikacji;
40. Stale monitorowanie konfiguracji w celu wykrycia odstępstw od ustalonych zasad bezpieczeństwa lub najlepszych praktyk;

c) **Wymagania licencyjne**

1. Licencja wieczysta (niewygasająca);
2. Oferowane licencje muszą pozwalać na użytkowanie oprogramowania zgodnie z przepisami prawa.
3. Licencja nie może ograniczać prawa licencjobiorcy do rozbudowy, zwiększenia ilości serwerów obsługujących oprogramowanie, przeniesienia oprogramowania na inny serwer, rozdzielenia funkcji serwera (osobny serwer bazy danych, osobny serwer aplikacji, osobny serwer plików).
4. Licencja musi być licencją bez ograniczenia ilości komputerów, serwerów, na których można zainstalować i używać oprogramowanie.
5. Licencja na oprogramowanie nie może w żaden sposób ograniczać sposobu pracy użytkowników końcowych (np. praca w sieci LAN, praca zdalna poprzez Internet).
6. Licencja nie może ograniczać prawa licencjobiorcy do wykonania kopii bezpieczeństwa oprogramowania w ilości, którą uzna za stosowną.
7. Licencja nie może ograniczać prawa licencjobiorcy do instalacji użytkowania oprogramowania na serwerach zapasowych uruchamianych w przypadku awarii serwerów podstawowych.
8. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do korzystania z oprogramowania na dowolnym komputerze klienckim (licencja nie może być przypisana do komputera/urządzenia).

d) **Zakres wdrożenia:**

1. Wdrożenie systemu ma być przeprowadzone w trzech etapach, obejmujących instalację, konfigurację oraz optymalizację detekcji zagrożeń w infrastrukturze IT.
2. Etap I:
    a) Wstępny audyt infrastruktury. Określenie liczby urządzeń i systemów (domenowych, pozadomenowych, agentowych i bezagentowych opartych na syslogu) koniecznych do połączenia z systemem SIEM. Oszacowanie priorytetów;
    b) Instalacja systemu na dostarczonym serwerze i wstępna konfiguracja
    c) Podłączenie urządzeń i systemów krytycznych infrastruktury IT do systemu SIEM. Konfiguracja agentów i urządzeń, aby przesyłały dane do systemu. Zabezpieczenie komunikacji;
    d) Zbieranie danych z systemów. Tworzenie bazy danych, na podstawie której możliwe będzie opracowanie reguł powiadomień o błędach i incydentach. Ustawienie zasad retencji zdarzeń oraz wielkości baz;
3. Etap II:
    a) Wdrożenie reguł wykrywania błędów i incydentów, na podstawie zebranych danych.;
    b) Implementacja reguł dla zapewnienie zgodności z przepisami NIST 800-53 oraz GDPR;

c) Implementacja reguł wspierających detekcję malware'u
d) Implementacja funkcji wykrywania podatności;
e) Wstępny tuning reguł. Dopracowywanie zasad, aby zgłaszały najważniejsze problemy;
f) Utworzenie dashboardu dla administratora przedstawiającego wykryte zagrożenia i problemy oraz kondycję infrastruktury IT;
g) Opracowanie raportów;

4. Etap III:
   a) Konfiguracja urządzeń i reguł pod komunikację z systemem SIEM
   b) Dopracowywanie reguł i automatyzacja zadań pod powstające problem
   c) Monitorowanie infrastruktury i reagowanie na powstające problemy;
   d) Przekazanie dokumentacji wdrożeniowej;
5. Etap IV:
   Wsparcie techniczne przez okres 1 roku od zakończenia wdrożenia;

e) **Szkolenie;**

Wykonawca przeprowadzi dla Zespołu IT Zamawiającego szkolenie warsztatowe z zakresu zarządzania systemem, z uwzględnieniem elementów takich jak:

1. Instalacja i konfiguracja systemu
2. Monitorowanie zdarzeń bezpieczeństwa i detekcja intruzji
3. Analiza logów i błędów
4. Integracja z innymi narzędziami i infrastrukturą
5. Praktyczne ćwiczenia i scenariusze użycia

IV. Serwer do klastra HA – 1 szt. – Typ II – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	Obudowa Rack o wysokości maksymalnie 1U z możliwością instalacji 8 dysków 2.5" NVMe;
Płyta główna	Obsługa procesorów 32 rdzeniowych. Szesnaście slotów przeznaczonych do instalacji pamięci. Obsługa do 1 TB pamięci RAM ECC DDR5 6400 MT/s;
Procesor	Zainstalowany procesor maksymalnie 32-rdzeniowy osiągający wynik 74 000 w teście PassMark CPU Mark – **załączyć do oferty wydruk** ze strony www.cpubenchmark.net lub www.passmark.com.
Pamięć RAM	256 GB DDR5 RDIMM 6400MT/s, moduły dwubankowe;
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający ○ Możliwość konfiguracji poziomów RAID: 0, 1, 10; ○ Wsparcie dla dysków SAS, SATA i NVMe; ○ Wsparcie dla PCIe gen. 4;
Dyski twarde	Zainstalowane 4 x 960 GB NVMe U2 do intensywnego odczytu
Gniazda PCI	Pięć slotów PCIe

Interfejsy sieciowe	2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)

Wbudowane porty	• 4 porty USB w tym min:
	  ○ 2 port USB 3.1 z tyłu obudowy,
	  ○ 1 port USB typu C z przodu obudowy
	• 1 port VGA
	• 1 x RJ45

Wentylatory	Redundantne, Hot-Plug
Zasilacz	Redundantny, Hot-Plug 1500W każdy, klasy Titanium;
Elementy montażowe	Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych
Bezpieczeństwo	1. Firmware podpisany kryptograficznie; 2. Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. 3. Sprzętowe szyfrowanie danych w stanie spoczynku, przechowywanych na dyskach na wypadek ich kradzieży; 4. Klucze szyfrujące muszą być przechowywane oddzielnie od danych; 5. Bezpieczny rozruch UEFI poprzez weryfikację podpisu cyfrowego komponentów rozruchowych przed załadowaniem systemu operacyjnego; 6. Wbudowany czujnik otwarcia obudowy; 7. Moduł TPM 2.0 8. Mechanizm umożliwiający weryfikację integralności firmware gwarantujący, że podczas rozruchu serwera ładowany jest wyłącznie autentyczny kod; 9. Możliwość usunięcia danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem; 10. Tryb blokady konfiguracji i aktualizacji oprogramowania sprzętowego. Po zablokowaniu systemu wszelkie próby zmiany konfiguracji muszą być blokowane. W przypadku próby zmiany krytycznych ustawień systemowych wyświetlany musi być komunikat o błędzie; 11. Automatyczne odzyskiwanie głównego obrazu BIOS/obrazu odzyskiwania
Karta zdalnego zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego karta zdalnego zarządzania, posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: 1. Zdalny dostęp do interfejsu graficznego serwera z dowolnego miejsca z przeglądarką internetową (wirtualna konsola) 2. Możliwość podłączenia obrazów ISO lub dysków USB w celu instalacji oprogramowania lub diagnostyki. 3. Śledzenie parametrów pracy serwera i generowanie powiadomień w przypadku wykrycia problemów. 4. Optymalizacja zużycia energii przez serwer. 5. Możliwość zdalnego uruchamiania i wyłączania serwera. 6. Uwierzytelnianie, autoryzacja i szyfrowanie danych; 7. zarządzanie serwerem za pomocą interfejsu graficznego przez przeglądarkę lub interfejsu wiersza poleceń (CLI); 8. Skanowanie BIOS-u musi weryfikować integralność i autentyczność obrazu BIOS-

	u;. Pomyślny wynik skanowania musi być rejestrowany w dzienniku kontrolera cyklu życia 9. Ochrona przed lukami w oprogramowaniu, próbami włamań i złośliwym oprogramowaniem. Proces systemowy, nie może uzyskać dostępu do plików ani sprzętu, które są poza jego zakresem; 10. Wsparcie dla SSH; 11. Szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika 12. Wirtualna konsola z dostępem do myszy, klawiatury 13. Wsparcie dla IPv6 14. Wsparcie dla SNMP; IPMI2.0, VLAN tagging, 15. Integracja z Active Directory 16. Wsparcie dla LLDP 17. Wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej 18. Możliwość podłączenia lokalnego poprzez złącze RS-232. 19. Automatyczne update firmware dla wszystkich komponentów serwera 20. Możliwość przywrócenia poprzednich wersji firmware 21. Możliwość eksportu/importu konfiguracji karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID do pliku XML lub JSON 22. Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych 23. Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram. 24. Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera 25. Serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej;
System operacyjny	Posiadający następujące, wbudowane funkcjonalności: 1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny system operacyjny. 3. 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. 4. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 6. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 7. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.

	8. 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). 9. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 10. Licencja musi uprawniać do zainstalowania systemu w środowisku fizycznym oraz na dwóch maszynach (instancjach) wirtualnych; 11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET 13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15. Dostępne dwa rodzaje graficznego interfejsu użytkownika: c) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, d) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18. 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), 19. 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.. 20. Oferowana licencja musi umożliwiać, zgodną z polityką licencyjną producenta system operacyjnego, pracę na serwerze wyposażonym w trzydzieści dwa rdzenie procesorowe; 21. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 22. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 23. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 24. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).

	25. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 26. 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 8.1. 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: • 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) 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) Wsparcie dla algorytmów Suite B (RFC 4869), l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputera m) 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: • 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) 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. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 30. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 31. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. Zorganizowany system szkoleń i materiały edukacyjne w języku polski
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 - **załączyć do oferty certyfikaty dla producenta;** • Oferowane urządzenie musi pochodzić z oficjalnego kanału dystrybucji producenta na rynek polski – **załączyć do oferty oświadczenie producenta;** • Aktywny certyfikat EPEAT dla Polski, co najmniej na poziomie SILVER, wydany nie wcześniej niż w roku 2024 – załączyć do oferty wydruk ze strony internetowej www.epeat.net – **załączyć do oferty;**
Gwarancja	• 36 miesięcy NBD on site producenta serwera; • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania, w tym także oprogramowania. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/portal) 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. • Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla da-

	nej naprawy zgodzi się na inną formę. • Uszkodzone dyski pozostają własnością zamawiającego;

V. System informatyczny zarządzający wykonywaniem kopii zapasowych wraz z wdrożeniem

a) Serwer Typ III – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Procesor	Musi osiągać 9100 w teście PassMark CPU Mark – **załączyć do oferty wydruk ze strony www.cpunechmark.net lub www.passmark.com;**
Obudowa	Maksymalnie 2U, rack;
Pamięć RAM	8 GB z możliwością rozbudowy do 64 GB;
Kieszenie na dyski	8 szt.
Pamięc flash	5 GB;
Obsługiwane dyski	2,5 cala SSD, 2,5 oraz 3,5 cala HDD, hot swap;
Porty / złącza	2 x 2,5G; 4 x USB 3.2; 2 x 10 GbE; 2 x M.2
Wentylacja	3 wentylatory pracujące w trybie pełnej prędkości, chłodzenia i cichym;
Zasilacz	Redundantny, 300W;
Zainstalowane dyski	8 x 4 TB SATA 6 Gb/s; Rozmiar sektora – 512e; Prędkość obrotowa – 7200 rpm. Rozmiar buforu – 256 MB; Prędkość przesyłu danych – 260 MB/s; Odczyt losowy – 150 IOPS; Zapis losowy - 400 IOPS; MTBF – 2 mln. godzin Gwarancja – 5 lat; Zużycie energii podczas odczytu/zapisu – maksymalnie 10W;
Zużycie energii	Maksymalnie 80W w trybie dostępu do danych;
Oprogramowanie	1. Pula SED o rozmiarze 300 TB 2. Liczba pul i woluminów – po 128 szt.; 3. Rozmiar woluminu i folderu udostępnianego – 250 TB; 4. Obsługa 512 udostępnionych folderów; 5. Możliwość rozszerzenia za pomocą jednostki JBOD producenta serwera; 6. Wsparcie dla Fibre Channel; 7. Obsługa grubego i cienkiego LUNu; 8. iSCSI LUN oparty na plikach i blokach; 9. Rozmiar LUN – 250 TB; 10. Obsługa 128 LUN; 11. Funkcje LUN: a) Przenoszenie LUN pomiędzy iSCSI i FC;

	b) Maskowanie LUN c) Import/eksport aliasów WWP d) Grupowanie portów FC; e) Wiązanie portu FC f) MPIO; g) Rozszerzenie pojemności LUN online h) Migawka, replikacja I klonowanie LUN;;
Warunki gwarancji	3 lata; Urządzenie musi pochodzić z autoryzowanego przez producenta kanału sprzedaży na rynek polski – **załączyć do oferty oświadczenie producenta;**
Wymagania dodatkowe	WoL; Obsługa ramek jumbo Zestaw do montażu w szafie rack; Funkcja WoL; Kabel zasilający – 2 szt. Kontrola przepływu; Agregacja łączy;

b) Serwer Typ IV – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	Obudowa Rack o wysokości maksymalnie 1U z możliwością instalacji 4 dysków 3.5” ; Z możliwością wyposażenia w panel LCD umieszczony na froncie, umożliwiający jednoznacznie stwierdzić, czy system działa poprawnie i pokazujący podstawowe stany działania serwera w tym adres IP karty zarządzającej;
Płyta główna	Obsługa procesorów 16 rdzeniowych. • 4 slotów przeznaczonych do instalacji pamięci. • obsługa do 128 GB pamięci RAM; • obsługa pamięci ECC DDR5;
Procesor	Zainstalowany procesor maksymalnie szesnastordzeniowy osiągający wynik 25 000 w teście PassMark CPU Mark – **załączyć do oferty wydruk** ze strony www.cpubenchmark.net lub www.passmark.com.
Pamięć RAM	128 GB DDR5 RDIMM 5600MT/s,
Kontroler RAID	• Sprzętowy kontroler dyskowy, posiadający: ○ Możliwość konfiguracji poziomów RAID: 0, 1, 10; ○ Możliwość autokonfiguracji; ○ Podłączenia 32 dysków/grup dysków wirtualnych w RAID; ○ 16 dysków wirtualnych w każdej grupie; ○ Wymiana urządzeń w trybie Hot-plug; ○ Wsparcie dla dysków SAS I SATA; ○ Obsługę PCIe gen. 4
Dyski twarde	Zainstalowane: 4 x dysk SATA o pojemności 12TB każdy, 7200 obr./min., Hot-Plug.
Gniazda PCI	Dwa sloty PCIe ;
Interfejsy	Wbudowane 2 interfejsy sieciowe 1Gb/s.

sieciowe	2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT; Karta SAS do podłączenia biblioteki taśmowej umożliwiająca przesył danych z prędkością 12G;

Wbudowane porty	• 4 porty USB w tym min.:
	  ○ 1 port USB 3.2 z tyłu obudowy,
	  ○ 1 port USB z przodu obudowy
	• 1 port VGA;
	• 1 serial port;

Zasilacze	Redundantne, Hot-Plug 700W każdy;
Elementy montażowe	Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych
Bezpieczeństwo	1. Firmware podpisany kryptograficznie; 2. Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. 3. Sprzętowe szyfrowanie danych w stanie spoczynku, przechowywanych na dyskach na wypadek ich kradzieży; 4. Klucze szyfrujące muszą być przechowywane oddzielnie od danych; 5. Bezpieczny rozruch UEFI poprzez weryfikację podpisu cyfrowego komponentów rozruchowych przed załadowaniem systemu operacyjnego; 6. Wbudowany czujnik otwarcia obudowy; 7. Moduł TPM 2.0 8. Mechanizm umożliwiający weryfikację integralności firmware gwarantujący, że podczas rozruchu serwera ładowany jest wyłącznie autentyczny kod; 9. Możliwość usunięcia danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem; 10. Tryb blokady konfiguracji i aktualizacji oprogramowania sprzętowego. Po zablokowaniu systemu wszelkie próby zmiany konfiguracji muszą być blokowane. W przypadku próby zmiany krytycznych ustawień systemowych wyświetlany musi być komunikat o błędzie; 11. Automatyczne odzyskiwanie głównego obrazu BIOS/obrazu odzyskiwania
Karta zdalnego zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego, posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: 1. Dostęp do interfejsu graficznego serwera z dowolnego miejsca z przeglądarką internetową (wirtualna konsola**)** 2. Możliwość podłączenia obrazów ISO lub dysków USB w celu instalacji oprogramowania lub diagnostyki. 3. Śledzenie parametrów pracy serwera i generowanie powiadomień w przypadku wykrycia problemów. 4. Optymalizacja zużycia energii przez serwer. 5. Możliwość zdalnego uruchamiania i wyłączania serwera. 6. Uwierzytelnianie, autoryzacja i szyfrowanie danych; 7. zarządzanie serwerem za pomocą interfejsu graficznego przez przeglądarkę lub interfejsu wiersza poleceń (CLI); 8. Skanowanie BIOS-u musi weryfikować integralność i autentyczność obrazu BIOS-

	u;. Pomyślny wynik skanowania musi być rejestrowany w dzienniku kontrolera cyklu życia 9. Ochrona przed lukami w oprogramowaniu, próbami włamań i złośliwym oprogramowaniem. Proces systemowy, nie może uzyskać dostępu do plików ani sprzętu, które są poza jego zakresem; 10. Wsparcie dla SSH; 11. Szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika 12. Wirtualna konsola z dostępem do myszy, klawiatury 13. Wsparcie dla IPv6 14. Wsparcie dla SNMP; IPMI2.0, VLAN tagging, 15. Integracja z Active Directory 16. Wsparcie dla LLDP 17. Wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej 18. Możliwość podłączenia lokalnego poprzez złącze RS-232. 19. Automatyczne update firmware dla wszystkich komponentów serwera 20. Możliwość przywrócenia poprzednich wersji firmware 21. Możliwość eksportu/importu konfiguracji karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID do pliku XML lub JSON 22. Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych 23. Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram. 24. Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera 25. Serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej;
System operacyjny	Musi posiadać następujące, wbudowane funkcjonalności:. 1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny system operacyjny. 3. 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. 4. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 6. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 7. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.

	8. 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). 9. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 10. Licencja musi uprawniać do zainstalowania systemu w środowisku fizycznym lub na dwóch maszynach (instancjach) wirtualnych; 11. Oferowana licencja musi umożliwiać, zgodną z polityką licencyjną producenta system operacyjnego, pracę na serwerze wyposażonym w maksymalnie szesnaście rdzeni procesorowych; 12. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 13. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET 14. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 15. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 16. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 17. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 18. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 19. Mechanizmy logowania w oparciu o: 20. Login i hasło, 21. Karty z certyfikatami (smartcard), 22. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 23. 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.. 24. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 25. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 26. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 27. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 28. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia

	aplikacji działających we wskazanych środowiskach. 29. 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: 30. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, 31. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, 32. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. 33. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1. 34. Zdalna dystrybucja oprogramowania na stacje robocze. 35. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej 36. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: a) Dystrybucję certyfikatów poprzez http b) Konsolidację CA dla wielu lasów domeny, c) Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, d) Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. 37. Szyfrowanie plików i folderów. 38. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). 39. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. 40. Serwis udostępniania stron WWW. 41. Wsparcie dla protokołu IP w wersji 6 (IPv6), 42. Wsparcie dla algorytmów Suite B (RFC 4869), 43. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach 44. 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: a) Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn

	wirtualnych, b) Obsługi ramek typu jumbo frames dla maszyn wirtualnych. c) Obsługi 4-KB sektorów dysków d) Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra 45. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. 46. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 47. 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. 48. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 49. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 50. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 51. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. 52. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 - **załączyć do oferty certyfikaty dla producenta;** • Oferowane urządzenie musi pochodzić z oficjalnego kanału dystrybucji producenta na rynek polski – **załączyć do oferty oświadczenie producenta;** • Aktywny certyfikat EPEAT dla Polski, co najmniej na poziomie SILVER, wydany nie wcześniej niż w roku 2024 – załączyć do oferty wydruk ze strony internetowej www.epeat.net – **załączyć do oferty;**
Gwarancja	• 36 miesięcy NBD on site producenta serwera; • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania, w tym także oprogramowania. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/portal) 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. • Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Uszkodzone dyski pozostają własnością zamawiającego;

c) Biblioteka taśmowa – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Technologia	LTO Ultrium wspierające technologię partycjonowania nośników. Urządzenie powinno mieć możliwość instalowania w tej samej obudowie także napędów LTO od generacji szóstej.
Wbudowany napęd	Napęd LTO-8 wyposażony w złącze SAS 6Gb; Oferowane urządzenie musi mieć możliwość instalowania i wykorzystania w tej samej obudowie także napędów LTO z interfejsem FC oraz wspierać technologię LTFS (Linear Tape File System). Zainstalowany napęd musi dynamicznie i płynnie dopasowywać prędkość zapisu do napływających danych (speed matching);
Ilość slotów i magazynki	8 slotów na nośniki podzielone na dwa magazynki w celu szybszego dostępu do danych i prostszego zarzadzania nośnikami i szybszej ich weryfikacji. Urządzenie powinno być dostarczone z kompletem magazynków. Wymagana ilość mail slot (I/E): 1. Możliwość zdalnego wysuwania magazynków poprzez web GUI
Pojemność	Bez kompresji – 48TB
Zarządzanie	Za pomocą panelu kontrolnego się na froncie urządzenia oraz zdalne przez sieć poprzez przeglądarkę internetową (web GUI; Wsparcie SNTP, protokołów SSL/TLS i IPv6 oraz definiowanie 4 poziomów zarządzania urządzeniem i dostępem do niego. Urządzenie musi mieć możliwość zabezpieczania swojej konfiguracji na podłączony, poprzez slot USB, penDrive. Operacja powinna być możliwa zarówna poprzez web GUI jak i poprzez panel kontrolny urządzenia. Możliwość zdalnego wysuwania magazynków, restartowania biblioteki oraz wyłączania zasilania napędów poprzez webGUI.
Dodatkowe interfejsy	Biblioteka musi być wyposażone w interfejs sieciowy, interfejs USB oraz ADI;
Obsługa urządzenia	Możliwość wymiany napędu, zasilacza i modułu portów zarządzania bez konieczności demontażu urządzenia z szafy przemysłowej oraz bez konieczności zdejmowania pokrywy głównej. Zarówno napęd jaki moduł interfejsów powinny być wyposażone w diody kontrolne, informujące o stanie technicznym;
Obudowa	Typu rack 19” o wysokości maksymalnie 1U. Wszystkie elementy do montażu muszą być dostarczone wraz z urządzeniem
Wyposażenie	Urządzenie musi być wyposażone w czytnik kodów kreskowych, kabel zasilający, kabel komunikacyjny konieczny do podłączenia urządzenia do odpowiedniego kontrolera serwera i umożliwiającego komunikację z urządzeniem – długość kabla min. 2m; Zestaw 4 nośników danych o pojemności 12 TB bez kompresji każdy wraz z nośnikiem czyszczącym – wszystkie nośniki z naklejkami z kodami kreskowymi
Warunki gwarancji	36 miesięcy gwarancji producenta biblioteki w miejscu instalacji

	urządzenia z czasem reakcji serwisu na zgłoszenia w ciągu 8 godzin. Czas przyjmowania zgłoszeń serwisowych w trybie 24x7. Przystąpienie do fizycznej naprawy najpóźniej w następnym dniu roboczym od zgłoszenia awarii z terminem naprawy najpóźniej do 48 godzin od rozpoczęcia. Możliwość rozszerzenia oferowanego serwisu producenta biblioteki do 84 miesięcy – **załączyć do oferty oświadczenie producenta**; Oferowane urządzenie musi być kompatybilne z oferowanym oprogramowaniem do wykonywania kopii zapasowej oraz pochodzić z autoryzowanego kanału sprzedaży producenta na rynek polski – **załączyć do oferty oświadczenie producenta urządzenia**;
Wdrożenie	Wdrożenie i szkolenie musi zostać przeprowadzone przez inżyniera dysponującego ugruntowaną wiedzą techniczną z zakresu administrowania oferowanym urządzeniem, potwierdzoną certyfikatem technicznym, wydanym przez producenta oferowanej biblioteki – **załączyć do oferty certyfikat potwierdzający;**

d) Oprogramowanie do wykonywania kopii zapasowych

1. Musi prawidłowo współpracować z oferowaną platformą wirtualizacyjną oraz systemami operacyjnymi zainstalowanymi na posiadanych przez zamawiającego komputerach I serwerach fizycznych oraz maszynach wirtualnych
2. Musi pozwalać na wykorzystanie dowolnego serwera oraz przestrzeni dyskowej (nie dedykowanych), za pośrednictwem protokołów CIFS lub NFS
3. Nie może wymagać instalacji dedykowanego agenta wewnątrz maszyny wirtualnej w celach backupu/przywracania
4. Nie może wymagać dodatkowej instalacji zewnętrznych aplikacji lub baz danych. Jeżeli oprogramowanie wymaga bazy danych musi ona być instalowana automatycznie z paczki opracowanej przez producenta i nie wymagać dodatkowych licencji). ;
5. Wszystkie funkcje i komponenty oprogramowania dla środowisk wirtualnych muszą być licencjonowane per gniazdo procesora w hostach wirtualizacyjnych służących za źródło backupu lub replikacji.
6. Licencje wieczyste bez terminu ważności
7. Licencja musi umożliwiać rozbudowę środowiska do 6 gniazd w hostach wirtualizacyjnych, 5 serwerów fizycznych ta powinna jednak umożliwiać rozbudowę do nie mniej niż 6 gniazd procesorów w obrębie środowiska
8. W ramach oferowanej licencji na określoną ilość gniazd procesorów wymagane jest zapewnienie 1 roku wsparcia technicznego producenta, zapewniającego dostęp do aktualizacji i poprawek oprogramowania oraz umożliwiającego kontakt z działem technicznym producenta w zakresie oferowanego oprogramowania
9. Licencja wieczysta, niewygasająca, na 2 gniazda procesorowe (sockety) w hostach wirtualizacyjnych, 3 serwery fizyczne i 80 komputerów fizycznych;
10. Wdrożenie oraz konfiguracja w obecności przedstawiciela Zamawiającego;
11. Oferent musi posiadać status autoryzowanego partnera producenta oprogramowania do wykonywania kopii zapasowej – **załączyć do Oferty certyfikat potwierdzający;**
12. Oprogramowanie musi posiadać funkcje wykonywania kopii zapasowych oraz ich replikacji, w tym co najmniej:

a) backup maszyn wirtualnych, serwerów I komputerów fizycznych;
b) replikację maszyn wirtualnych (tworzenie i aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych);

13. Możliwość przesłania pierwszych kopii za pośrednictwem dysków zewnętrznych do lokalizacji docelowej oraz późniejsze wznowienie ochrony maszyn wirtualnych
14. Możliwość określania pasma wykorzystywanego przez oprogramowanie do backupu globalnie lub per zadanie
15. Możliwość tworzenia do 100 punktów przywracania dla każdej z maszyn wirtualnych w ramach zadania backup
16. Obsługa retencji zgodnie z zasadą grandfather-father-son;
17. Oprogramowanie musi pozwalać na rotację punktów przywracania w trybie dziennym, tygodniowym, miesięcznym oraz rocznym
18. Kopia backupu (replikacja) do innych repozytoriów backupu lokalnych oraz zdalnych
19. Oprogramowanie musi pozwalać na utworzenie kopii źródłowego repozytorium backupu oraz tylko wybranych backupów. Kopia tworzona musi być zgodnie z określonym harmonogramem
20. Oprogramowanie musi pozwalać na określenie kolejności, w jakiej są backupowane lub replikowane maszyny wirtualne w ramach zadania
21. Oprogramowanie musi umożliwiać tworzenie scenariuszy odtwarzania w środowiskach wirtualnych składających się z wielu etapów np. wyłączenia/włączenia maszyny, odczekania określonego czasu, wykonania jednego lub wielu wcześniej utworzonych zadań backupu lub replikacji
22. Oprogramowanie musi udostępniać widok kalendarza z naniesionymi zadaniami backupu/replikacji w celu łatwiejszego zarządzania zadaniami;
23. Oprogramowanie musi posiadać poniższe funkcje pozwalające na ograniczenie wielkości backupowanych danych:
    a) deduplikacja backupu, działająca w ramach całego repozytorium backupu oraz obejmująca wszystkie dane, które są w tym repozytorium przechowywań
    b) Kompresja backupu, w tym konfigurowalny stopień kompresji
    c) Automatyczne pomijanie plików i partycji wymiany w systemach operacyjnych działających jako maszyny wirtualne
24. Oprogramowanie musi posiadać poniższe funkcje, gwarantujące spójność danych:
    a) Spójny backup i replikacja maszyn wirtualnych z systemami Windows i Linux
    b) Wykonywanie własnych skryptów przed wykonaniem backupu oraz po jego wykonaniu
    c) Automatyczne usuwanie (trunking) logów transakcyjnych;:
    d) Automatyczna weryfikacja utworzonych backupów oraz replik poprzez uruchamianie maszyny wirtualnej bezpośrednio z backupu lub uruchamianie repliki
25. Oprogramowanie musi pozwalać na generowanie oraz automatyczne wysyłanie raportów ze zrzutami ekranu testowanych maszyn wirtualnych;
26. Pełna weryfikacja wszystkich danych przechowywanych w repozytorium backupu na żądanie, ze wskazaniem niespójnych punktów przywracania
27. Szyfrowanie danych przesyłanych przez sieć do zdalnego repozytorium backupu i/lub repozytorium replikacji
28. Oprogramowanie musi posiadać poniższe funkcje:
    a) Blokowanie złośliwego oprogramowania przed zainstalowaniem;
    b) Podejście default deny do wszystkich plików;
    c) Uruchamianie nieznanych plików w odizolowanym środowisku;

d) Host Intrusion Prevention System (HIPS);
e) Możliwosc cofnięcia podejrzanej zmiany
f) Analiza zachowań oparta na chmurze;
g) Wykrywanie i usuwanie zagrożeń typu spyware;
h) Kontrola aplikacji;
i) Biała lista;
j) Alerty bezpieczeństwa;
k) Konfigurowalna ochrona
l) Przywracanie pełnych maszyn wirtualnych z backupu do oryginalnego lub innego serwera wirtualizacji
m) Uruchomienie maszyny wirtualnej bezpośrednio z plików backupu w środowisku (bez wcześniejszego przywracania);
n) Przywracanie pojedynczych plików czy folderów bezpośrednio z plików backupu bez wcześniejszego przywracania całej maszyny wirtualnej;
o) Przywracanie pojedynczych obiektów z poniższych aplikacji bez wcześniejszego przywracania całej maszyny wirtualnej z backupu czy rozpakowywania plików backupu):
   - MS Active Directory
   - MS SQL
p) Migracja dysków maszyn wirtualnych pomiędzy środowiskami wirtualizacyjnymi;

29. Oprogramowanie musi pozwalać na:
    a) Tworzenie backupu i replik przyrostowo;
    b) Wykonywanie backupów przyrostowych bez wymogu okresowego tworzenia kopii pełnych
    c) Akceleracje sieciową umożliwiającą redukcję ilości danych przesyłanych w Sieci
    d) Wsparcie dla urządzeń oferujących dodatkową deduplikację danych;
    e) Wizualne wykonywanie komendy ping;
    f) Wyświetlanie scieżki I mierzenie opóźnienia przesyłu pakietów przez sieć IP;
    g) Wysyłanie zapytań i uzyskiwanie informacji o dominie i adresie najbliższego serwera DNS;
    h) Skanowanie zakresu adresów IP w poszukiwaniu aktywnych węzłów które wymagają aktualizacji lub wyłączenia;
    i) Wyświetlanie adresów MAC dla poszczególnych adresów IP;
    j) Identyfikacja dostawców kart sieciowych na podstawie znanych prefiksów MAC;
    k) Wysyłanie pakietów WoL do wybranego węzła sieci;
    l) Obliczanie liczby sieci IPv4 na podstawie parametrów maski sieciowej;
    m) Wykrywanie usług UDP, TCP I TLS działajacych w sieci, Możliwość skanowania podsieci lub pojedynczego urządzenia;
    n) Weryfikacja informacji SNMP w sieci. Obsługa wszystkich wersji SNMP
30. Oprogramowanie musi pozwalać na następujące formy zarządzania:
    a) Interfejs web do zarządzania wszystkimi aspektami związanymi z backupem i przywracaniem danych
    b) Wysyłanie powiadomień email dotyczących wykonywanych zadań backupu, błędów, cyklicznych raportów;
    c) Wysyłanie powiadomień email potwierdzających poprawność odtworzenia maszyn wirtualnych dla wybranych zadań w formie zrzutów ekranu z uruchomionej z backupu maszyny wirtualnej
31. Zadanie backupu musi mieć możliwość uruchamiania zgodnie z harmonogramem, z opcją dodawania wielu harmonogramów dla pojedynczego zadania

32. Pliki backupu muszą mieć możliwość eksportu z opcją wyboru rodzaju dysków do których będzie robiony eksport.
33. Oprogramowanie musi pozwalać na eksportowanie oraz importowanie konfiguracji w celu reinstalacji i migracji
34. Oprogramowanie musi umożliwiać integrację z Active Directory
35. Oprogramowanie musi wspierać tryb multi tenant, umożliwiający podzielenie oprogramowania do backupu na kilka instancji zarządzanych z odrębnych interfejsów;

VII. Instalacja, konfiguracja, wdrożenie zakupionego sprzętu i oprogramowania;

W ramach wdrożenia wykonawca będzie zobowiązany do wykonania następującego zakresu prac:

1. Integracja dostarczonych urządzeń z infrastrukturą zamawiającego
2. Montaż zakupionych urządzeń w szafach serwerowych oraz uporządkowanie/organizacja okablowania i spięcie urządzeń kablami sieciowymi
3. Instalacja serwerów, w tym:
   a) Aktualizacja sterowników do podzespołów oraz BIOS serwera;
   b) Instalacja i konfiguracja oprogramowania serwerowego, w tym systemu operacyjnego, oprogramowania bazodanowego i wirtualizacyjnego;,
   c) Konfiguracja zabezpieczeń
   d) Konfiguracja usług aktualizacyjnych
4. Utworzenie klastra wysokiej dostępności z serwera dostarczonego w ramach realizacji niniejszego zamówienia oraz udostępnionego przez zamawiającego;
5. Konfiguracja i uruchomienie klastra;
6. Konfiguracja do wykonywania kopii zapasowych dla klastra wysokiej dostępności;
   a) Instalacja oprogramowania do backupu na dedykowanych serwerach oraz serwerach wirtualizacyjnych, o ile wymaga tego dostarczone oprogramowanie;
   b) Instalacja oprogramowania klienckiego na backupowanych komputerach;
   c) Wykonanie planu kopii zapasowych serwerów i komputerów;
   d) Konfiguracja zabezpieczeń
   e) Instalacja i konfiguracja biblioteki taśmowej
7. Instalacja i konfiguracja systemu SIEM na dostarczonym klastrze HA;
8. Instalacja i konfiguracja przełączników sieciowych w tym:
   a) Konfiguracja usług;
   b) Konfiguracja zabezpieczeń
   c) Wydzielenie podsieci VLAN;
9. Opis architektury technicznej (komponentów sprzętowych, systemowych)

Zamawiający zastrzega sobie możliwość wezwania oferentów, którzy złożyli oferty niepodlegające odrzuceniu w niniejszym postępowaniu, do okazania zaoferowanego sprzętu i oprogramowania, w celu sprawdzenia ich zgodności z wymaganiami określonymi przez Zamawiającego w SWZ.
Okazanie nastąpi w dniu wyznaczonym przez Zamawiającego, po terminie składania ofert. Zamawiający poinformuje o terminie przeprowadzenia okazania z co najmniej pięciodniowym wyprzedzeniem (dni kalendarzowe).
Niestawienie się oferenta w wyznaczonym czasie i miejscu na okazaniu (prezentacji) sprzętu i/lub oprogramowania, uznane będzie jako negatywny wynik okazania, tj. niepotwierdzenie przez oferenta

wymagań określonych przez Zamawiającego, co będzie skutkowało odrzuceniem oferty na podstawie art. 226 ust. 1 pkt. 5 Ustawy Pzp.