

Załącznik nr 5a do SWZ

WZP.271.16.2026.AA.MT

Zamawiający :
Gmina Nowogard
Plac Wolności 1
72-200 Nowogard

.....

 (nazwa oraz adres Wykonawcy)

Przedmiotowe środki dowodowe składane celem potwierdzenia zgodnościz
opisem przedmiotu zamówienia w postępowaniu pn:

Dostawa i wdrożenie sprzętu informatycznego oraz modernizacja istniejącego
środowiska informatycznego wraz z podniesieniem poziomu
cyberbezpieczeństwa w ramach konkursu grantowego „Cyberbezpieczny
Samorząd” w trzech jednostkach Gminy Nowogard

SERWER TYP 1 (2 sztuki)

Parametr	Charakterystyka (wymagania minimalne)	Parametry oferowane
Obudowa	<ul style="list-style-type: none"> Obudowa Rack o wysokości max 2U 16 wnęk na dyski 2.5" 	
	<ul style="list-style-type: none"> Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. 	Kryterium oceny ofert NIE – 0 punktów TAK – 6 punktów
Płyta główna	<ul style="list-style-type: none"> Płyta główna z możliwością zainstalowania do dwóch procesorów. Obsługa procesorów 144 rdzeniowych. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. Na płycie głównej powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 8TB pamięci RAM. 	
Procesor	<ul style="list-style-type: none"> Zainstalowane dwa procesory min. 8-rdzeniowe, min. 3.7GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 170 w teście SPECspeed®2017_fp_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej oferowanego serwera. 	

RAM	<ul style="list-style-type: none"> 128GB DDR5 RDIMM 6400MT/s, 	
Kontroler RAID	<ul style="list-style-type: none"> Sprzętowy kontroler dyskowy, posiadający <ul style="list-style-type: none"> Min. 8GB nieulotnej pamięci cache, Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących Obsługa dysków 22.5 Gbps SAS, 12 Gbps SAS, and 6 Gbps SATA/SAS 	
Dyski twarde	<ul style="list-style-type: none"> Zainstalowane: <ul style="list-style-type: none"> 2x dysk SSD SATA o pojemności min. 480GB, Hot-Plug Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1. 	
Gniazda PCI	<ul style="list-style-type: none"> Cztery sloty PCIe Dwa sloty OCP 	
Interfejsy sieciowe/FC/SAS	<ul style="list-style-type: none"> 4 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) Dwuportowa karta sieciowa 25Gb Ethernet w standardzie SFP28 Dwuportowa karta 32GB FC HBA 	
Wbudowane porty	<ul style="list-style-type: none"> 4 porty USB w tym min: <ul style="list-style-type: none"> 1 port USB 2.0 Type-C 2 porty USB 3.1 1 port USB 3.0 wewnątrz obudowy Port VGA z tyłu obudowy 	
Video	<ul style="list-style-type: none"> Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 	
Zasilacze	<ul style="list-style-type: none"> Redundantne, Hot-Plug min. 1500W klasy Titanium 	
Elementy montażowe	<ul style="list-style-type: none"> Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych 	
System operacyjny/dodatkowe oprogramowanie	<p>Microsoft Windows Server 2025 Datacenter lub rozwiązanie równoważne. Przez rozwiązanie równoważne Zamawiający rozumie system operacyjny zapewniający co najmniej:</p> <ul style="list-style-type: none"> pełną obsługę usług Active Directory Domain Services (AD DS), obsługę usług DNS oraz DHCP, obsługę zasad grup (Group Policy), możliwość pracy jako kontroler domeny Active Directory, 	

	<ul style="list-style-type: none"> • obsługę środowiska wirtualizacji Hyper-V lub rozwiązania równoważnego, • obsługę funkcji Failover Clustering, • obsługę funkcji Storage Replica, • możliwość uruchamiania nieograniczonej liczby instancji wirtualnych systemu operacyjnego zgodnie z zasadami licencjonowania producenta, • integrację z usługami katalogowymi Active Directory, • współpracę z bazami danych Microsoft SQL Server, • współpracę z systemami SIEM, NAC oraz rozwiązaniami monitoringu przewidzianymi w projekcie, • możliwość centralnego zarządzania aktualizacjami systemowymi, • możliwość integracji z mechanizmami uwierzytelniania wieloskładnikowego (MFA), • możliwość pracy w środowisku kopii zapasowych oraz odtwarzania awaryjnego wdrażanym w ramach projektu. • Licencjonowanie systemu operacyjnego musi zostać dobrane w sposób zapewniający zgodne z warunkami producenta uruchomienie wszystkich maszyn wirtualnych przewidzianych do wdrożenia w środowisku Urzędu Miejskiego. 	
Bezpieczeństwo	<ul style="list-style-type: none"> • Zatrzaszk górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • 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 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).	
	<ul style="list-style-type: none"> Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera 	Kryterium oceny ofert NIE – 0 punktów TAK – 6 punktów
Karta Zarządzania	<ul style="list-style-type: none"> Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające: <ul style="list-style-type: none"> zdalny dostęp do graficznego interfejsu Web karty zarządzającej szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika wsparcie dla IPv6 wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH Wsparcie dla automatycznej rejestracji DNS wsparcie dla LLDP możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy. Monitorowanie zużycia dysków SSD Możliwość przywrócenia poprzednich wersji firmware możliwość rozszerzenia funkcjonalności o: <ul style="list-style-type: none"> integracja z Active Directory możliwość podmontowania zdalnych wirtualnych napędów wirtualną konsolę z dostępem do myszy, klawiatury możliwość obsługi przez sześciu administratorów jednocześnie wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer Możliwość wykrywania odchyłeń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera Automatyczne zgłaszanie alertów do centrum serwisowego producenta Automatyczne update firmware dla wszystkich komponentów serwera 	

	<ul style="list-style-type: none"> możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram. możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych narzędzi analitycznych jak Splunk, Grafana, Elasticsearch możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielokrotnego przy logowaniu do karty zarządzającej Automatyczne odświeżanie certyfikatów SSL monitorowanie przepływu powietrza na bieżąco (w CFM) 	
Oprogramowanie do zarządzania	<ul style="list-style-type: none"> Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: <ul style="list-style-type: none"> Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych integracja z Active Directory Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram Szczegółowy opis wykrytych systemów oraz ich komponentów Możliwość eksportu raportu do CSV, HTML, XLS, PDF Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. Grupowanie urządzeń w oparciu o kryteria użytkownika Tworzenie automatycznie grup urządzeń w oparciu o 	Kryterium oceny ofert NIE – 0 punktów TAK – 6 punktów

	<p>dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji</p> <ul style="list-style-type: none"> ○ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach ○ Szybki podgląd stanu środowiska ○ Podsumowanie stanu dla każdego urządzenia ○ Szczegółowy status urządzenia/elementu/komponentu ○ Generowanie alertów przy zmianie stanu urządzenia. ○ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń ○ Integracja z service desk producenta dostarczonej platformy sprzętowej ○ Możliwość przejęcia zdalnego pulpitu ○ Możliwość podmontowania wirtualnego napędu ○ Kreator umożliwiający dostosowanie akcji dla wybranych alertów ○ Możliwość importu plików MIB ○ Przesyłanie alertów „as-is” do innych konsol firm trzecich ○ Możliwość definiowania ról administratorów ○ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów ○ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) ○ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta ○ Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów ○ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. ○ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. ○ Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile ○ Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. ○ Tworzenie gotowych paczek informacji umożliwiających 	
--	---	--

	<p>zdiagnozowanie awarii urządzenia przez serwis producenta.</p> <ul style="list-style-type: none"> ○ Zdalne uruchamianie diagnostyki serwera. ○ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. ○ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi. ○ Integracja z środowiskiem VMware vCenter pozwalająca z konsoli/plugin: <ul style="list-style-type: none"> ▪ wykonać zautomatyzowaną aktualizację firmware serwerów w klastrze Vmware do zdefiniowanej polityki poziomu mikrokodów ▪ wykonać/zweryfikować konfigurację serwera zgodną ze zdefiniowaną polityką konfiguracji ▪ z konsoli vCenter uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny) ▪ inwentaryzacja komponentów w serwerze i ich mikrokodów ▪ historia poboru mocy i temperatury serwera ▪ zbieranie danych diagnostycznych serwera do paczki serwisowej 	
Oprogramowanie do monitorowania	<p>Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:</p> <ul style="list-style-type: none"> ● Monitoring: <ul style="list-style-type: none"> ○ ilość podłączonych oraz rozłączonych systemów ○ stan podłączonych urządzeń ○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów ○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia ○ informacje o statusie gwarancji dla poszczególnych urządzeń ○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń ○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. ○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych ○ Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów 	<p>Kryterium oceny ofert NIE – 0 punktów TAK – 6 punktów</p>

	<p>historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych.</p> <ul style="list-style-type: none"> ○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. ○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. ○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. ○ Monitoring parametrów serwerów z informacją o minimum: <ul style="list-style-type: none"> ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ○ Monitoring parametrów pamięci masowych z informacją o minimum: <ul style="list-style-type: none"> ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów ○ Monitoring parametrów przełączników sieciowych z informacją o minimum: <ul style="list-style-type: none"> ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ▪ Stanie komponentów: zasilacze, wentylatory ▪ Podłączonych hostach 	
--	--	--

	<ul style="list-style-type: none"> ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Aktualizacja firmware <ul style="list-style-type: none"> ○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty <ul style="list-style-type: none"> ○ Możliwość generowania raportów dla serwerów zawierających informację o: <ul style="list-style-type: none"> ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, ○ Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: <ul style="list-style-type: none"> ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji ○ Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo <ul style="list-style-type: none"> ○ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. ○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. 	
--	--	--

	<ul style="list-style-type: none"> ○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. ○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. ● Wspierane urządzenia <ul style="list-style-type: none"> ○ Urządzenie Producenta dostarczane w ramach postępowania ○ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) ● Wirtualny asystent <ul style="list-style-type: none"> ○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; ● Możliwość rozszerzenia funkcjonalności <ul style="list-style-type: none"> ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. ● Inne <ul style="list-style-type: none"> ○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android 	
Certyfikaty	<ul style="list-style-type: none"> ● Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 ● Serwer musi posiadać deklaracja CE. ● 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, dla kraju, w którym produkt będzie użytkowany, według normy wprowadzonej w 2019 roku - Wykonawca 	

	złożyć dokument potwierdzający spełnianie wymogu. <ul style="list-style-type: none"> Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025. 	
Dokumentacja użytkownika	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. Możliwość bezpłatnego pobierania aktualizacji firmware, BIOS i sterowników po wygaśnięciu gwarancji. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego 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. 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 	

	<p>bezpieczeństwa cybernetycznego.</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> ○ Możliwości utworzenia zgłaszania 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 przekaże 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. • 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. 	
--	---	--

UWAGA!

Należy złożyć wraz z ofertą.

Dokument należy wypełnić i podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym.

Załącznik nr 5b do SWZ

WZP.271.16.2026.AA.MT

Zamawiający :
Gmina Nowogard
Plac Wolności 1
72-200 Nowogard

.....

 (nazwa oraz adres Wykonawcy)

Przedmiotowe środki dowodowe składane celem potwierdzenia zgodnościz
opisem przedmiotu zamówienia w postępowaniu pn:

Dostawa i wdrożenie sprzętu informatycznego oraz modernizacja istniejącego
środowiska informatycznego wraz z podniesieniem poziomu
cyberbezpieczeństwa w ramach konkursu grantowego „Cyberbezpieczny
Samorząd” w trzech jednostkach Gminy Nowogard

SERWER TYP 2 (1 sztuka)

Parametr	Charakterystyka (wymagania minimalne)	Parametry oferowane
Obudowa	<ul style="list-style-type: none"> Obudowa Rack o wysokości max 2U 16 wnęk na dyski 2.5" 	
	<ul style="list-style-type: none"> Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. 	Kryterium oceny ofert NIE – 0 punktów TAK – 3 punkty
Płyta główna	<ul style="list-style-type: none"> Płyta główna z możliwością zainstalowania do dwóch procesorów. Obsługa procesorów 144 rdzeniowych. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. Na płycie głównej powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 8TB pamięci RAM. 	
Procesor	<ul style="list-style-type: none"> Zainstalowane dwa procesory min. 8-rdzeniowe, min. 3.7GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 170 w teście SPECspeed®2017_fp_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej oferowanego serwera. 	

RAM	<ul style="list-style-type: none"> 128GB DDR5 RDIMM 6400MT/s, 	
Kontroler RAID	<ul style="list-style-type: none"> Sprzętowy kontroler dyskowy, posiadający <ul style="list-style-type: none"> Min. 8GB nieulotnej pamięci cache, Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących Obsługa dysków 22.5 Gbps SAS, 12 Gbps SAS, and 6 Gbps SATA/SAS 	
Dyski twarde	<ul style="list-style-type: none"> Zainstalowane: <ul style="list-style-type: none"> 2x dysk SSD SATA o pojemności min. 480GB, Hot-Plug 4x dysk SAS o pojemności min. 2.4TB, Hot-Plug Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1. 	
Gniazda PCI	<ul style="list-style-type: none"> Cztery sloty PCIe Dwa sloty OCP 	
Interfejsy sieciowe/FC/SAS	<ul style="list-style-type: none"> 4 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) Dwuportowa karta sieciowa 25Gb Ethernet w standardzie SFP28 	
Wbudowane porty	<ul style="list-style-type: none"> 4 porty USB w tym min: <ul style="list-style-type: none"> 1 port USB 2.0 Type-C 2 porty USB 3.1 1 port USB 3.0 wewnątrz obudowy Port VGA z tyłu obudowy 	
Video	<ul style="list-style-type: none"> Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 	
Zasilacze	<ul style="list-style-type: none"> Redundantne, Hot-Plug min. 1500W klasy Titanium 	
Elementy montażowe	<ul style="list-style-type: none"> Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych 	
System operacyjny/dodatkowe oprogramowanie	<p>Microsoft Windows Server 2025 Standard lub Datacenter lub rozwiązanie równoważne.</p> <p>W przypadku zaoferowania systemu Microsoft Windows Server 2025 Standard liczba dostarczonych licencji musi zostać dobrana w sposób zapewniający, zgodnie z zasadami licencjonowania producenta, możliwość legalnego uruchomienia minimum 8 maszyn wirtualnych w środowisku CUS i ZEAS.</p>	

	<p>W przypadku zaoferowania systemu Microsoft Windows Server 2025 Datacenter liczba dostarczonych licencji musi zostać dobrana w sposób zapewniający zgodne z warunkami producenta uruchomienie wszystkich maszyn wirtualnych przewidzianych do wdrożenia.</p> <p>Przez rozwiązanie równoważne Zamawiający rozumie system operacyjny zapewniający co najmniej:</p> <ul style="list-style-type: none"> • pełną obsługę usług Active Directory Domain Services (AD DS), • obsługę usług DNS oraz DHCP, • obsługę zasad grup (Group Policy), • możliwość pracy jako kontroler domeny Active Directory, • obsługę środowiska wirtualizacji Hyper-V lub rozwiązania równoważnego, • obsługę funkcji Failover Clustering, • obsługę funkcji Storage Replica, • integrację z usługami katalogowymi Active Directory, • współpracę z bazami danych Microsoft SQL Server, • współpracę z systemami SIEM, NAC oraz rozwiązaniami monitoringu przewidzianymi w projekcie, • możliwość centralnego zarządzania aktualizacjami systemowymi, • możliwość integracji z mechanizmami uwierzytelniania wieloskładnikowego (MFA), • możliwość pracy w środowisku kopii zapasowych oraz odtwarzania awaryjnego wdrażanym w ramach projektu. 	
Bezpieczeństwo	<ul style="list-style-type: none"> • Zatrzaszk górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • 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).	
	<ul style="list-style-type: none"> Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera 	Kryterium oceny ofert NIE – 0 punktów TAK – 3 punkty
Karta Zarządzania	<ul style="list-style-type: none"> Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające: <ul style="list-style-type: none"> zdalny dostęp do graficznego interfejsu Web karty zarządzającej szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika wsparcie dla IPv6 wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH Wsparcie dla automatycznej rejestracji DNS wsparcie dla LLDP możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy. Monitorowanie zużycia dysków SSD Możliwość przywrócenia poprzednich wersji firmware możliwość rozszerzenia funkcjonalności o: <ul style="list-style-type: none"> integracja z Active Directory możliwość podmontowania zdalnych wirtualnych napędów wirtualną konsolę z dostępem do myszy, klawiatury możliwość obsługi przez sześciu administratorów jednocześnie wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer Możliwość wykrywania odchyłeń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera 	

	<ul style="list-style-type: none"> ○ Automatyczne zgłaszanie alertów do centrum serwisowego producenta ○ Automatyczne update firmware dla wszystkich komponentów serwera ○ możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer ○ możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe ○ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer ○ Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON ○ Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych ○ Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram. ○ możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych narzędzi analitycznych jak Splunk, Grafana, Elasticsearch ○ możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielokrotnego przy logowaniu do karty zarządzającej ○ Automatyczne odświeżanie certyfikatów SSL ○ monitorowanie przepływu powietrza na bieżąco (w CFM) 	
Oprogramowanie do zarządzania	<ul style="list-style-type: none"> • Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: <ul style="list-style-type: none"> ○ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych ○ integracja z Active Directory ○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta ○ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish ○ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram ○ Szczegółowy opis wykrytych systemów oraz ich komponentów ○ Możliwość eksportu raportu do CSV, HTML, XLS, 	Kryterium oceny ofert NIE – 0 punktów TAK – 3 punkty

	<p>PDF</p> <ul style="list-style-type: none"> Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. Grupowanie urządzeń w oparciu o kryteria użytkownika Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach Szybki podgląd stanu środowiska Podsumowanie stanu dla każdego urządzenia Szczegółowy status urządzenia/elementu/komponentu Generowanie alertów przy zmianie stanu urządzenia. Filtry raportów umożliwiające podgląd najważniejszych zdarzeń Integracja z service desk producenta dostarczonej platformy sprzętowej Możliwość przejęcia zdalnego pulpitu Możliwość podmontowania wirtualnego napędu Kreator umożliwiający dostosowanie akcji dla wybranych alertów Możliwość importu plików MIB Przesyłanie alertów „as-is” do innych konsol firm trzecich Możliwość definiowania ról administratorów Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd 	
--	---	--

	<p>pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.</p> <ul style="list-style-type: none"> ○ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. ○ Wdrażanie serwerów, rozwiązań modułarnych oraz przełączników sieciowych w oparciu o profile ○ Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. ○ Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. ○ Zdalne uruchamianie diagnostyki serwera. ○ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. ○ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. ○ Integracja z środowiskiem VMware vCenter pozwalająca z konsoli/plugin: <ul style="list-style-type: none"> ▪ wykonać zautomatyzowaną aktualizację firmware serwerów w klastrze Vmware do zdefiniowanej polityki poziomu mikrokodów ▪ wykonać/zweryfikować konfigurację serwera zgodną ze zdefiniowaną polityką konfiguracji ▪ z konsoli vCenter uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny) ▪ inwentaryzacja komponentów w serwerze i ich mikrokodów ▪ historia poboru mocy i temperatury serwera ▪ zbieranie danych diagnostycznych serwera do paczki serwisowej 	
Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać	Kryterium oceny ofert NIE – 0 punktów TAK – 3 punkty

	<p>następujące funkcjonalności:</p> <ul style="list-style-type: none"> • Monitoring: <ul style="list-style-type: none"> ○ ilość podłączonych oraz rozłączonych systemów ○ stan podłączonych urządzeń ○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów ○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia ○ informacje o statusie gwarancji dla poszczególnych urządzeń ○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń ○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. ○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych ○ Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. ○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. ○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. ○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. ○ Monitoring parametrów serwerów z informacją o minimum: <ul style="list-style-type: none"> ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie 	
--	--	--

	<p>generowana informacja o anomaliach.</p> <ul style="list-style-type: none"> ○ Monitoring parametrów pamięci masowych z informacją o minimum: <ul style="list-style-type: none"> ▪ Opóźnień ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów ○ Monitoring parametrów przełączników sieciowych z informacją o minimum: <ul style="list-style-type: none"> ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ▪ Stanie komponentów: zasilacze, wentylatory ▪ Podłączonych hostach ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ● Aktualizacja firmware <ul style="list-style-type: none"> ○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizacji firmware, dla systemów 	
--	--	--

	<p>przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania</p> <ul style="list-style-type: none"> ○ możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania <ul style="list-style-type: none"> • Raporty <ul style="list-style-type: none"> ○ Możliwość generowania raportów dla serwerów zawierających informację o: <ul style="list-style-type: none"> ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, ○ Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: <ul style="list-style-type: none"> ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji ○ Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo <ul style="list-style-type: none"> ○ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. ○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. ○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. ○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia <ul style="list-style-type: none"> ○ Urządzenie Producenta dostarczane w ramach postępowania ○ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego 	
--	--	--

	<p>urządzenia (jeśli takie są w posiadaniu Zamawiającego)</p> <ul style="list-style-type: none"> • Wirtualny asystent <ul style="list-style-type: none"> ◦ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności <ul style="list-style-type: none"> ◦ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne <ul style="list-style-type: none"> ◦ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android 	
Certyfikaty	<ul style="list-style-type: none"> • Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • 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, dla kraju, w którym produkt będzie użytkowany, według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu. • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025. 	
Dokumentacja	<ul style="list-style-type: none"> • Zamawiający wymaga dokumentacji w języku polskim lub 	

użytkownika	<p>angielskim.</p> <ul style="list-style-type: none"> Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. 	
Warunki gwarancji	<ul style="list-style-type: none"> Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. Możliwość bezpłatnego pobierania aktualizacji firmware, BIOS i sterowników po wygaśnięciu gwarancji. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego 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. 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 	

	<p>Zamawiającego.</p> <ul style="list-style-type: none"> Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: <ul style="list-style-type: none"> Możliwości utworzenia zgłaszania 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 przekaże 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. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. 	
--	---	--

UWAGA!

Należy złożyć wraz z ofertą.

Dokument należy wypełnić i podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym.

Załącznik nr 5c do SWZ

WZP.271.16.2026.AA.MT

Zamawiający :
Gmina Nowogard
Plac Wolności 1
72-200 Nowogard

.....

 (nazwa oraz adres Wykonawcy)

Przedmiotowe środki dowodowe składane celem potwierdzenia zgodnościz
opisem przedmiotu zamówienia w postępowaniu pn:

Dostawa i wdrożenie sprzętu informatycznego oraz modernizacja istniejącego
środowiska informatycznego wraz z podniesieniem poziomu
cyberbezpieczeństwa w ramach konkursu grantowego „Cyberbezpieczny
Samorząd” w trzech jednostkach Gminy Nowogard

MACIERZ DYSKOWA (1 sztuka)

Parametr	Charakterystyka (wymagania minimalne)	
Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19", o wysokość maksymalnie 2U z możliwością instalacji min. 12 dysków 3.5"	
Przestrzeń dyskowa	Zainstalowane: 7x dysk SAS o pojemności min. 12TB, Hot-Plug 4x dysk SSD SAS o pojemności min. 1.92TB, Hot-Plug	
Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 264 dysków twardej.	
Obsługa dysków	Macierz musi mieć możliwość obsługi dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5" jak również 3,5".	
Sposób zabezpieczenia danych	Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping). Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku).	



	Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.	
Tryb pracy kontrolerów w macierzowych	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.	
Pamięć cache	Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.	
Rozbudowa pamięci cache	Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.	
Interfejsy	Macierz musi posiadać, co najmniej 8 portów 32Gb FC (4 porty na kontroler)	
Kable/wkładki	8x wkładka 32Gb FC	
Zarządzanie	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.	
Zarządzanie grupami dyskowymi i oraz dyskami logicznymi	Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.	
Thin Provisioning	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP). Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.	
Tiering	Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS.	



	<p>Tiering musi obejmować wszystkie woluminy w danej puli dyskowej. Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.</p>	
Wewnętrzne kopie migawkowe	<p>Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii.</p> <p>Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.</p>	
Wewnętrzne kopie pełne	<p>Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych.</p> <p>Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.</p>	
Migracja danych w obrębie macierzy	<p>Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.</p>	
Zdalna replikacja danych	<p>Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy.</p> <p>Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem.</p>	
Podłączanie zewnętrznych systemów operacyjnych	<p>Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami).</p> <p>Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix.</p> <p>Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów</p>	



	operacyjnych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.	
Redundancja	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. Zasilacze użyte w macierzy powinny spełniać wymagania dotyczące sprawności dla zasilacza minimum 80+ Gold.	
Monitoring	Rozwiązanie w obszarze monitoringu musi zapewniać automatyczną ocenę kondycji środowiska macierzy na podstawie wskaźnika health score wraz z prezentacją rekomendowanych działań korygujących, ciągły monitoring konfiguracji bezpieczeństwa (w tym wykrywanie odchyłeń od dobrych praktyk i ocenę ich wpływu na ryzyko), predykcyjne wykrywanie anomalii w teledziennym z wykorzystaniem mechanizmów analitycznych/ML, centralny widok ryzyka dla całej floty macierzy z możliwością rankingu i filtrowania systemów, nadzór nad łącznością oraz integralnością danych teledziennych (z generowaniem alertów przy przerwach lub niekompletności danych), analizę zużycia energii i parametrów środowiskowych pod kątem ryzyka operacyjnego, a także generowanie raportów oceny bezpieczeństwa środowiska, zawierających listę odchyłeń i rekomendowane działania prewencyjne lub naprawcze.	
Dodatkowe wymagania	Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych. Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.	
Standardy bezpieczeństwa	Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union), IEC 60950-1 (International). Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające spełnienie powyższych zaleceń.	
Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Oferowany model macierzy w momencie składania oferty nie może mieć ogłoszonej daty końca sprzedaży. Na żądanie Zamawiającego,	

	<p>Wykonawca musi przedstawić oświadczenie producenta oferowanego urządzenia, potwierdzające brak ogłoszenia takiej daty.</p> <p>Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001.</p> <p>Deklaracja zgodności CE.</p>	
Warunki gwarancji	<p>Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat.</p> <p>Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet.</p> <p>Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.</p> <p>Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.</p> <p>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.</p> <p>Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.</p> <p>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.</p> <p>Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.</p> <p>Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:</p> <ul style="list-style-type: none"> • Możliwości utworzenia zgłaszania 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 	

	<p>Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.</p> <ul style="list-style-type: none">• 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 przekaże 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. <p>Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.</p>	
--	---	--

UWAGA!

Należy złożyć wraz z ofertą.

Dokument należy wypełnić i podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym.

Załącznik nr 5d do SWZ

WZP.271.16.2026.AA.MT

Zamawiający :
Gmina Nowogard
Plac Wolności 1
72-200 Nowogard

.....

 (nazwa oraz adres Wykonawcy)

Przedmiotowe środki dowodowe składane celem potwierdzenia zgodnościz
opisem przedmiotu zamówienia w postępowaniu pn:

Dostawa i wdrożenie sprzętu informatycznego oraz modernizacja istniejącego
środowiska informatycznego wraz z podniesieniem poziomu
cyberbezpieczeństwa w ramach konkursu grantowego „Cyberbezpieczny
Samorząd” w trzech jednostkach Gminy Nowogard

UPS CENTRALNY (1 sztuka)

Parametr	Charakterystyka (wymagania minimalne)	
Opis zasilacza UPS	Projektuje się zasilacz UPS pracujący w topologii on-line VFI-SS-111, wg normy IEC 62040-3, o mocy 20kVA/20kW. UPS będzie wyposażony w wewnętrzny, bezprzerwowy bypass elektroniczny. Bypass wewnętrzny będzie posiadał zabezpieczenie przed zwrotnym podawaniem energii do sieci zasilającej (backfeed protection, zgodnie z normą IEC 62040). UPS będzie zasilany dwutorowo – przez tor główny (układ prostownik-falownik) oraz tor rezerwowy (bypass elektroniczny). Dodatkowo będzie wyposażony w zewnętrzny tor obejściowy (serwisowy, mechaniczny). Baterie akumulatorów, zapewniające czas podtrzymania 6 minut dla obciążenia 20kW, będą umieszczone wewnątrz zasilacza UPS.	
Opis techniczny	<ul style="list-style-type: none"> • producent oferowanego urządzenia powinien posiadać certyfikat ISO 9001 w zakresie projektowania, produkcji, sprzedaży i serwisu systemów zasilania gwarantowanego UPS • moc wyjściowa: 20 kVA/20 kW • możliwość pracy równoległej do 4 jednostek • ilość faz 3/3 – trzy fazy wejściowe i trzy fazy wyjściowe • sprawność w trybie on-line: minimum 95,64% w zakresie obciążenia 50-100% (do 99,08% w trybie oszczędzania energii) • tolerancja napięcia wejściowego prostownika, bez przejścia na pracę z baterii: 190/330-276/478 V przy obciążeniu 100%; 	

	<ul style="list-style-type: none"> • częstotliwość wejściowa 50 Hz lub 60 Hz z tolerancją 40 Hz do 72 Hz • $\cos\phi$ wyjściowy = 1 • $\cos\phi$ wejściowy = 0,99 przy 100% obciążenia • współczynnik szczytu: 3:1 • zabezpieczenie przed zwrotnym podaniem energii do sieci zasilającej (backfeed protection, zgodnie z normą IEC 62040) w torze bypassu statycznego UPS • urządzenie powinno być wyposażone w system nieciągłego ładowania baterii. Należy dołączyć opis sposobu zarządzania pracą baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta • wejściowe zniekształcenia THDi < 3% • wyjściowe THDu: <ul style="list-style-type: none"> - dla obciążenia liniowego < 2% - dla obciążenia nieliniowego < 5% • Urządzenie musi posiadać panel komunikacyjny, w którym powinny być zainstalowane: <ul style="list-style-type: none"> - gniazdo komunikacji RS-232 - gniazdo wyłącznika awaryjnego p.poż. • interfejs komunikacyjny SNMP – obsługiwane protokoły: IPv4/v6, TLS, SNMPv1/v3, DHCP, SSH, LDAP prędkość gigabit'owa (half-duplex, full-duplex). Zgodność z normami dot. cyberbezpieczeństwa UL 2900-1 lub IEC62443-4-2. Opcjonalnie: Modbus TCP/RTU • graficzny wyświetlacz LCD 	
Wymiary	Wymiary UPS (szer. x gł. x wys.): 380 x 740 x 1328 mm	

UWAGA!

Należy złożyć wraz z ofertą.

Dokument należy wypełnić i podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym.