



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Cyberbezpieczny
Samorząd

Załącznik nr 1A

Załącznik do wypełnienia przez Wykonawcę

Wypełniony załącznik należy obowiązkowo złożyć wraz z ofertą.

Szczegółowy opis przedmiotu zamówienia - specyfikacja techniczna oferowanego sprzętu

„Dostawa sprzętu IT wraz z oprogramowaniem w ramach projektu grantowego "Cyberbezpieczny Samorząd" –

Obszar techniczny -część 2

współfinansowanego ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II „Zaawansowane usługi cyfrowe” Działanie 2.2 „Wzmocnienie krajowego systemu cyberbezpieczeństwa”, tytuł projektu: **„Przygotowanie Gminy Borów do przeciwdziałania zagrożeniom cyberbezpieczeństwa oraz doskonalenie świadomości w zakresie zagrożeń bezpieczeństwa w cyberprzestrzeni”.**

UWAGA!

Przed wypełnieniem zapoznać się z informacjami dodatkowymi zamieszczonymi na końcu niniejszego dokumentu

KOD CPV - 48820000-2 - Serwery

I. SERWER - 1 KPL

L.P	Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry
1	OBUDOWA	<ul style="list-style-type: none"> Obudowa Rack o wysokości 2U 8 wnęk na dyski 3.5" Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, pozwalający jednoznacznie stwierdzić, czy system działa poprawnie i pokazujący podstawowe stany działania serwera w tym adres IP karty zarządzającej <p>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.</p>	<p>SPEŁNIA TAK / NIE</p> <p>Producent</p> <p>Model wersja</p>



2	Płyta główna	<ul style="list-style-type: none"> Płyta główna z możliwością zainstalowania do dwóch procesorów. Obsługa procesorów 32 rdzeniowych. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. Na płycie głównej powinno znajdować się 16 slotów przeznaczonych do instalacji pamięci. <p>Płyta główna powinna obsługiwać do 1TB pamięci RAM.</p>	SPEŁNIA TAK / NIE
3	Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych	SPEŁNIA TAK / NIE
4	Procesor	Zainstalowany jeden procesor min. 8-rdzeniowy, min. 2.6GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 169 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.	SPEŁNIA TAK / NIE
5	Pamięć RAM	64 GB DDR5 RDIMM 5600 MT/s	SPEŁNIA TAK / NIE
6	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 samo szyfrujących 	SPEŁNIA TAK / NIE
7	Dyski twarde	<p>Zainstalowane:</p> <ul style="list-style-type: none"> 4x dysk SAS o pojemności min. 2.4TB, Hot-Plug Zainstalowane dwa dyski M.2 NVMe SSD o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. 	SPEŁNIA TAK / NIE
8	Gniazda PCI	Dwa sloty PCIe	SPEŁNIA TAK / NIE
9	Interfejsy sieciowe/FC/SAS	<p>Wbudowane 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)</p> <p>Dwuportowa karta sieciowa 10Gb Ethernet w standardzie BaseT</p>	SPEŁNIA TAK / NIE
10	Wbudowane porty	<ul style="list-style-type: none"> 4 porty USB w tym min: <ul style="list-style-type: none"> 1 port USB 3.0 z tyłu obudowy, 1 port micro USB z przodu obudowy 2 port VGA z czego jeden z przodu obudowy Możliwość rozbudowy o port RS232 	



11	Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024	SPEŁNIA TAK / NIE
12	Wentylatory	Redundantne, Hot-Plug	SPEŁNIA TAK / NIE
13	Zasilacze	Redundantne, Hot-Plug min. 700W klasy Titanium	SPEŁNIA TAK / NIE
14	Elementy montażowe	Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych	SPEŁNIA TAK / NIE
15	System operacyjny/dodatkowe oprogramowanie	<ul style="list-style-type: none"> Windows Server 2025 Standard lub równoważne – licencja dobrana tak, aby umożliwić uruchomienie 4 maszyn wirtualnych lub równoważne 30x Windows Server 2025/2022 Device CALs lub równoważne 	SPEŁNIA TAK / NIE
16	Bezpieczeństwo	<ul style="list-style-type: none"> Zatrask górnej pokrywy oraz blokada na ramce panelu 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 <p>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).</p>	SPEŁNIA TAK / NIE



17	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 możliwość podmontowania zdalnych wirtualnych napędów wirtualną konsolę z dostępem do myszy, klawiatury wsparcie dla IPv6 wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer integracja z Active Directory możliwość obsługi przez ośmiu administratorów jednocześnie Wsparcie dla automatycznej rejestracji DNS wsparcie dla LLDP wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej możliwość podłączenia lokalnego poprzez złącze RS-232. możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy. Monitorowanie zużycia dysków SSD możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi, Automatyczne zgłaszanie alertów do centrum serwisowego producenta Automatyczne update firmware dla wszystkich komponentów serwera Możliwość przywrócenia poprzednich wersji firmware Możliwość 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 wykrywania odchyłeń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera Serwer musi posiadać możliwość uruchomienia funkcjonalności umożliwiającej dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu 	SPEŁNIA TAK / NIE
----	-------------------	--	-------------------



		<p>dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE lub WIFI.</p> <p>Możliwość rozszerzenia funkcjonalności karty o:</p> <ul style="list-style-type: none"> 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 kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania Automatyczne odświeżanie certyfikatów SSL możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielokrotnego przy logowaniu do karty zarządzającej możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe monitorowanie przepływu powietrza na bieżąco (w CFM) 	
18	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 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 	SPEŁNIA TAK / NIE



		<ul style="list-style-type: none"> o Podsumowanie stanu dla każdego urządzenia o Szczegółowy status urządzenia/elementu/komponentu o Generowanie alertów przy zmianie stanu urządzenia. o Filtry raportów umożliwiające podgląd najważniejszych zdarzeń o Integracja z service desk producenta dostarczonej platformy sprzętowej o Możliwość przejęcia zdalnego pulpitu o Możliwość podmontowania wirtualnego napędu o Kreator umożliwiający dostosowanie akcji dla wybranych alertów o Możliwość importu plików MIB o Przesyłanie alertów „as-is” do innych konsol firm trzecich o Możliwość definiowania ról administratorów o Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów o Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) o Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta o Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów o Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informacje o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. o Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. o Wdrażanie serwerów, rozwiązań modułarnych oraz przełączników sieciowych w oparciu o profile o Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. o Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. o Zdalne uruchamianie diagnostyki serwera. o Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. o Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. 	
--	--	--	--



19	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 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 generowana informacja o anomaliach. ○ Monitoring parametrów pamięci masowych z informacją o minimum: <ul style="list-style-type: none"> ▪ Opóźnieniach 	SPEŁNIA TAK / NIE
----	--	---	-------------------



		<ul style="list-style-type: none"> ▪ 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 snapshot'ów ○ 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 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. ○ 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 <p>Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android</p>	
--	--	---	--



20	Gwarancja oraz wsparcie	<ol style="list-style-type: none"> 1. Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres minimum 3 lat. 2. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. 3. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. 4. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. 5. 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. 6. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. 7. 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. 8. 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. 9. Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: 10. Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. 11. 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. 12. Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. 13. 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. 14. 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. 	SPEŁNIA TAK / NIE
----	--------------------------------	--	-------------------



		<p>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> <p>15. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.</p> <p>16. 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.</p>	
21	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 według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu. <p>Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.</p>	SPEŁNIA TAK / NIE



22	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.	SPEŁNIA TAK / NIE
23	Wdrożenie	<ol style="list-style-type: none">1. Zakres przedmiotu zamówienia obejmuje wykonanie instalacji, uruchomienie, wdrożenie oraz konfigurację systemów/licencji zgodnie z wymaganiami Zamawiającego lub najlepszymi praktykami oraz doświadczeniem Dostawcy. Ponadto, Dostawca zobowiązuje się do przeprowadzenia szkolenia dla co najmniej jednego pracownika Zamawiającego w zakresie obsługi systemów/licencji przy czym ukończenie szkolenia zostanie potwierdzone odpowiednim certyfikatem lub zaświadczeniem2. Oprogramowanie systemowe musi być zainstalowane3. Serwery wirtualne uruchomione zgodnie z wytycznymi zamawiającego i gotowe do instalacji oprogramowania zamawiającego	SPEŁNIA TAK / NIE

**II. SERWER NAS z dyskami do kopii zapasowych wraz z oprogramowaniem do wykonywania kopii zapasowych - 1 KPL**

L.P	Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry
1	Obudowa	Rack 2U o wymiarach maksymalnych 88 mm x 490 mm x 560mm + przesuwane szyny do montażu w szafie rack	SPEŁNIA TAK / NIE Producent Model wersja
2	Procesor	Procesor co najmniej 4-rdzeniowy, 8-wątkowy min. 3.35 GHz	SPEŁNIA TAK / NIE
3	Pamięć RAM	8GB DDR4 ECC UDIMM RAM z możliwością rozszerzenia do 32GB	SPEŁNIA TAK / NIE
4	Ilość obsługiwanych dysków	12 dysków 3,5" lub 2,5" SATA HDD/SSD, z możliwością rozszerzenia o dodatkową półkę 12 dyskową.	SPEŁNIA TAK / NIE
5	Ilość dysków zamontowanych	8 dysków 3,5" o pojemności 8 TB, prędkości obrotowej 5400RPM, rozmiarze buforu 256MB, 1mln h MTBF, gwarancja producenta co najmniej 36 mieś., dyski powinny być zgodne z listą kompatybilności oraz pochodzić od tego samego producenta co urządzenie.	SPEŁNIA TAK / NIE
6	Interfejsy sieciowe	4 porty 1GbE RJ-45	SPEŁNIA TAK / NIE
7	Porty	2 porty USB 3.2 1. generacji 1 gniazdo rozszerzenia (eSATA) 1x PCIe 4-liniowe gniazdo x8 generacji 3	SPEŁNIA TAK / NIE
8	Wskaźniki LED	Zasilanie, alert, status, LAN, HDD1-4	SPEŁNIA TAK / NIE
9	Obsługa RAID	Synology Hybrid RAID (SHR), Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6 i RAID 10	SPEŁNIA TAK / NIE
10	Protokoły	SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP i VPN (PPTP, OpenVPN™, L2TP)	SPEŁNIA TAK / NIE



11	Usługi/ oprogramowanie do backupu	<p>Licencja wieczysta z serwisem do 30.06.2026 r. do backupu 30 komputerów, 4 serwerów fizycznych, 4 maszyn wirtualnych</p> <ol style="list-style-type: none"> 1. Pełne wsparcie dla systemów rodziny Microsoft Windows od wersji 10 wzwyż, Microsoft Server od wersji 2019 wzwyż 2. Pełne wsparcie dla systemów Red Hat Enterprise Linux 8 and 7, CentOS 7, Ubuntu 20.04, 18.04, 16.04, 3. Pełne wsparcie dla środowisk wirtualnych co najmniej Hyper-V 2016 I wzwyż, VMware 6.7 wzywyż I innych 4. Wsparcie dla 32 i 64-bitowych systemów Microsoft. 5. Wsparcie systemów plików: FAT16, FAT16X, FAT32, FAT32X, NTFS. 6. Wsparcie dla dysków z tablicą partycji MBR oraz GPT 7. Program i wsparcie techniczne dostępne w języku polskim 8. Możliwość instalacji na hostach fizycznych, maszynach wirtualnych, kontenerach docker. <p>Zarządzanie i magazyny</p> <ol style="list-style-type: none"> 1. Produkt dostępny w polskiej wersji językowej. 2. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej 3. System musi umożliwiać tworzenie kopii zapasowych na poziomie dysków 4. System musi umożliwiać tworzenie kopii zapasowych na poziomie plików i folderów 5. System musi umożliwiać replikację kopii zapasowych do wielu lokalizacji docelowych 6. System musi umożliwiać tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT 7. System musi umożliwiać współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft 8. Możliwość zdefiniowania limitu przepustowości sieciowej z jakiej ma korzystać oprogramowanie backupowe 9. System zarządzania nie może być oparty o relacyjne bazy danych. 10. Rozwiązanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej). 11. Rozwiązanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera (urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera (urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów). 	SPEŁNIA TAK / NIE
----	--------------------------------------	--	-------------------



		<ol style="list-style-type: none"> 12. Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania, ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych. 13. Rozwiązanie musi być systemem multi-storage-owym i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako przestrzeń do replikacji danych. 14. System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykl. 15. Rozwiązanie w warstwie sprzętowej powinno bazować na standardowych komponentach architektury x86, bez powiązania i polegania na komponentach wyłącznie jednego dostawcy (tzw. "no proprietary vendor lock"). 16. System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami. 17. System musi umożliwiać wykonywanie kopii obrazu dysku, kopii plików i katalogów oraz kopii maszyn wirtualnych bez ich zatrzymywania z zachowaniem stuprocentowej integralności i spójności danych wewnątrz wykonanej kopii zapasowej. 18. Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie. 19. Rozwiązanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia. 20. System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu. 21. Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych 22. Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS. 23. System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego. 24. System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii). 	
--	--	---	--



		<p>25. Rozwiązanie musi udostępniać możliwość podglądu postępu działania dowolnego zadania, w tym zadania wykonywania kopii zapasowych, odtwarzania danych, testowego odtwarzania danych, usuwania danych oraz zadania odświeżania zajętości magazynu na dane.</p> <p>26. Rozwiązanie musi posiadać system powiadamiania poprzez e-mail oraz Slack o zdarzeniach w następujących przypadkach: zadanie zostało zakończone pomyślnie, zadanie zostało zakończone z ostrzeżeniami, zadanie zostało zakończone z błędem, zadanie zostało anulowane, zadanie nie zostało uruchomione.</p> <p>27. System powinien umożliwiać wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika,</p> <p>28. Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta.</p> <p>29. Rozwiązanie musi być wyskalowane, dobrane pod względem wymaganej funkcjonalności i wydajności stosownie do ilości zabezpieczanych danych i obiektów z uwzględnieniem przyrostu danych (serwery, maszyny wirtualne, bazy danych itp.) zgodnie z opisem w zapytaniu ofertowym.</p> <p>30. Wydajność oferowanej konfiguracji musi być taka, aby wszystkie funkcje systemu były dostępne w chwili wdrożenia (np. deduplikacja, kompresja, instancja workerów i browserów, replikacja, testowe odtwarzanie maszyn wirtualnych).</p> <p>31. System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych.</p> <p>32. Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów.</p> <p>33. Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych z deduplikowanych</p> <p>34. Proces deduplikacji nie może posiadać pojedynczego punktu awarii, tym samym musi być dostępny jednocześnie na każdym wspieranym magazynie na dane - również replikacyjnych. Awaria jednego z magazynów na dane nie może wpłynąć na integralność deduplikatów, jak i tablicy deduplikatów na innym magazynie.</p> <p>35. Proces deduplikacji realizowany jest blokiem o stałej wielkości, którego wielkość może zostać ustalona na etapie wdrożenia rozwiązania zgodnie z najlepszymi praktykami producenta.</p> <p>36. Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego.</p>	
--	--	--	--



		<p>37. Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki.</p> <p>38. Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu.</p> <p>Środowiska fizyczne i bazy danych</p> <ol style="list-style-type: none"> 1. Rozwiązanie powinno umożliwiać tworzenie grup urządzeń w celu automatyzacji procesów podczas pracy z urządzeniami. 2. Produkt musi posiadać możliwość tworzenia zadań dla grupy urządzeń oraz dla wybranych urządzeń. 3. Rozwiązanie musi pozwalać na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej. 4. Rozwiązanie backupowe musi pozwalać na zabezpieczanie zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption. 5. System jest niezależny od wersji Microsoft SQL i musi umożliwiać przywracanie danych SQL dla tej samej lub nowszej wersji. 6. System musi obsługiwać również narzędzia RMAN firmy Oracle do tworzenia kopii zapasowych i odzyskiwania. Dodatkowo system musi obsługiwać funkcję przyrostowego scalania danych. 7. System kopii zapasowej musi wspierać odtwarzanie pojedynczych plików z systemów Windows oraz Linux. 8. W przypadku niedostępności źródła danych, system musi oczekiwać na powrót dostępności źródła danych przez określony przez administratora okres. W przypadku braku powrotu dostępności źródła, system musi podjąć ustaloną przez administratora liczbę prób kontynuacji kopii. W przypadku powrotu źródła danych system musi kontynuować zadanie backupu od momentu, w którym wystąpiła niedostępność źródła - system nie może rozpoczynać zadania od punktu początkowego i rozpoczynać przesyłania kopii od zera. W przypadku braku powrotu źródła danych system powinien zakończyć zadanie błędem. 9. Odtwarzanie Bare Metal Restore w Systemie może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika. 	
--	--	---	--



10. Rozwiązanie powinno umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego bootowalnego nośnika danych.
11. Rozwiązanie powinno wspierać odtwarzanie danych w scenariuszach P2P, P2V, V2P, V2V.
12. Rozwiązanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK).
13. Rozwiązanie musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) oraz z prawami dostępu. Funkcjonalność ta musi być możliwa do skonfigurowania przez administratora na etapie konfiguracji procesu przywracania danych.
14. Rozwiązanie musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows).

Środowiska wirtualne

1. System musi wspierać kopię w trybie application-aware dla wszystkich wspieranych wirtualizatorów.
2. System musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowanie zaawansowanych metod transportu (HotAdd, SAN, LAN), w tym metodami LAN-Free, tj. takimi, które podczas wykonywania backupu nie obciążają interfejsów sieciowych maszyn wirtualnych.
3. System kopii zapasowej musi wykorzystywać mechanizmy Change Block Tracking oraz Replica Change Tracking dla wspieranych przez producenta platformach wirtualizacyjnych.
4. Rozwiązanie producenta musi być certyfikowane przez dostawcę platformy wirtualizacyjnej, tj. producent musi uczestniczyć w programie Technology Alliance Partner.
5. System kopii zapasowej musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage-u użytego do przechowywania kopii zapasowych.
6. Dla środowiska vSphere i Hyper-V rozwiązanie powinno umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).
7. System kopii zapasowej musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere.
8. System kopii zapasowej musi umożliwiać weryfikację odtwarzalności wirtualnych maszyn według własnego harmonogramu w dowolnym środowisku.



		<p>Aplikacje SaaS</p> <ol style="list-style-type: none"> 1. Ochrona z tej samej konsoli dla Microsoft 365 minimum na poziomie, skrzynek pocztowych, OneDrive, kontaktów, kalendarza. 2. Rozwiązanie musi umożliwiać przywracanie danych Microsoft 365: do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku .pst oraz do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji) 3. System musi umożliwiać granularne odtwarzanie danych, tj. pojedynczych plików z kopii obrazu dysku oraz pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365. 4. System musi umożliwiać zabezpieczanie środowisk Git, w tym GitHub, GitLab oraz Bitbucket wraz z metadanymi 5. System musi umożliwiać odtworzenie dowolnego środowiska Git w dowolnym innym środowisku Git, tzw. odtwarzanie crossowe. 6. System musi umożliwiać zabezpieczenie metadanych zebranych wokół repozytorium w ramach zabezpieczanego środowiska Git. 7. System musi umożliwiać odtwarzanie metadanych repozytorium Git do dowolnego innego środowiska Git w przypadku chęci odtworzenia repozytorium. 8. System musi umożliwiać zabezpieczenie środowisk Jira 9. System musi umożliwiać odtworzenie środowiska Jira do chmury lub środowiska lokalnego. 10. System musi umożliwiać zabezpieczenie środowisk Jira <p>Licencjonowanie i wsparcie techniczne</p> <ol style="list-style-type: none"> 1. Wszystkie linie supportu muszą być obsługiwane w języku polskim. 2. Wsparcie techniczne musi być świadczone bezpośrednio przez główną siedzibę producenta. 3. Możliwość zgłaszania ticketów supportowych bezpośrednio z poziomu interfejsu zarządzania w formie czatu. 4. Producent wraz z rozwiązaniem musi udostępnić materiały samopomocowe w j. polskim (minimum dostęp do bazy wiedzy, materiałów wideo oraz kart produktów) 5. Wsparcie techniczne musi umożliwiać korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego. 6. Licencje w ramach rozwiązania powinny pozwalać na zabezpieczenie określonej przez Zamawiającego ilości hostów w obrębie wspieranych przez System środowisk. 7. Licencje powinny być dostępne w opcji wieczystej . 	
--	--	---	--



		<p>8. Dostęp do wsparcia technicznego producenta powinno obowiązywać przez okres do 30.06.2025 r,</p> <p>9. Sposób licencjonowania opiera się na:</p> <ul style="list-style-type: none"> - ilości serwerów/endpointów - dla fizycznych urządzeń, - ilości socketów w hostach - dla środowisk wirtualnych lub ilości maszyn wirtualnych, - ilość repozytoriów - dla GIT. <p>10. Licencje powinny umożliwiać zabezpieczenie w wersji wieczystej/subskrybcyjnej:</p> <ul style="list-style-type: none"> - 30 stacji roboczych, - 4 serwer fizyczny, - 4 serwerów wirtualnych <p>Anty-ransomware i bezpieczeństwo</p> <ol style="list-style-type: none"> 1. System plików rozwiązania musi być odporny na ataki Ransomware (zapewnić ochronę przed szyfrowaniem end-to-end, kopie zapasowe nie mogą być nadpisywane - "niezmienny system plików"). 2. System powinien umożliwiać wykorzystanie wbudowanego menedżera haseł do przechowywania wszelkich sekretów (haseł, danych dostępowych, kluczy szyfrujących) wykorzystywanych przez System 3. System powinien umożliwiać przywrócenie hasła głównego administratora w przypadku jego utraty. 4. W ramach systemu, komunikacja pomiędzy hostem źródłowym, a magazynem powinna odbywać się tylko i wyłącznie bezpośrednio pomiędzy agentem backupu, a magazynem. Komunikacja nie może przechodzić przez serwer backupu, ani żaden inny komponent, którego awaria sparaliżowałaby działanie Systemu. System nie może posiadać pojedynczego punktu awarii. <p>System musi działać w zgodzie z regułą Zero-knowledge Encryption. Oznacza to, że wszelkie sekrety muszą być przechowywane w centralnym Managerze Haseł w postaci zaszyfrowanej algorytmem AES i być udostępniane agentowi dopiero w momencie rozpoczęcia wykonywania kopii zapasowej. Sekrety nie mogą być przechowywane w konfiguracji agenta na zabezpieczonym urządzeniu.</p>	
--	--	---	--



12	Szkolenia	<p>Szkolenie musi zostać przeprowadzone przez Producenta systemu w siedzibie zamawiającego.</p> <p>Powinno zawierać zagadnienia :</p> <ol style="list-style-type: none"> 1. Instalację i konfigurację oprogramowania do backupu pkt.11 SWZ: <ul style="list-style-type: none"> o Zapoznanie z procesem instalacji różnych komponentów systemu (np. serwerów backupowych, agentów na stacjach roboczych). o Konfiguracja podstawowych ustawień aplikacji oraz dostosowanie ich do specyficznych potrzeb organizacji. 2. Zarządzania politykami backupowymi: <ul style="list-style-type: none"> o Tworzenie i modyfikowanie polityk backupowych dla różnych środowisk (wirtualnych, fizycznych, chmurowych). o Określanie harmonogramów tworzenia kopii zapasowych, retencji danych, oraz polityk dostępu. 3. Monitoring i raportowanie: <ul style="list-style-type: none"> o Przegląd narzędzi do monitorowania procesów backupowych i odzyskiwania danych. o Tworzenie raportów i analiz, które pomagają w audytach i zapewniają pełną kontrolę nad procesami ochrony danych. 4. Odnowienie i odzyskiwanie danych: <ul style="list-style-type: none"> o Szkolenie w zakresie przywracania danych z kopii zapasowych, zarówno na poziomie całych systemów, jak i pojedynczych plików. o Omówienie różnych scenariuszy odzyskiwania, takich jak odzyskiwanie po awarii, po ataku ransomware, czy w przypadku awarii sprzętu. 5. Bezpieczeństwo i zarządzanie użytkownikami: <ul style="list-style-type: none"> o Implementacja mechanizmów bezpieczeństwa, takich jak szyfrowanie danych, kontrola dostępu oraz zarządzanie rolami użytkowników. o Ochrona przed zagrożeniami zewnętrznymi i wewnętrznymi, w tym weryfikacja integralności kopii zapasowych. 	SPEŁNIA TAK / NIE
13	Obsługa migawek	<ul style="list-style-type: none"> • Maksymalna liczba migawek na foldery współdzielone: 1 024 • Maksymalna liczba migawek systemu: 65 536 	SPEŁNIA TAK / NIE
14	Zarządzanie dyskami	SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów,	SPEŁNIA TAK / NIE
15	Język GUI	Polski	SPEŁNIA TAK / NIE
16	Gwarancja i serwis	Minimum 3 lata gwarancji (z możliwością rozszerzenia do 5 lat – dodatkowe kryterium punktowane zgodnie z SWZ)	SPEŁNIA TAK / NIE
17	Certyfikaty	FCC, CE, BSMI., VCCI, RCM, UKCA, EAC, CCC, KC, UL	SPEŁNIA TAK / NIE
18	System plików	<p>Wewnętrzny: Btrfs, ext4</p> <p>Zewnętrzny: Btrfs, ext4, ext3, FAT32, NTFS, HFS+, exFAT</p>	SPEŁNIA TAK / NIE



19	Liczba wolumenów	do 64	SPEŁNIA TAK / NIE
20	Liczba iSCSI Targetów	do 128	SPEŁNIA TAK / NIE
21	Liczba iSCSI LUN	do 256	SPEŁNIA TAK / NIE
22	Liczba kont użytkowników	min. 2048	SPEŁNIA TAK / NIE
23	Liczba grup	min. 256	SPEŁNIA TAK / NIE
24	Liczba udziałów	mon. 512	SPEŁNIA TAK / NIE
25	Ilość jednoczesnych połączeń	500 dla CIFS/AFP/NFS/FTP/WebDAV; 2,000 po rozszerzeniu RAM	SPEŁNIA TAK / NIE
26	Chłodzenie	Co najmniej 3 wentylatory	SPEŁNIA TAK / NIE
27	Wdrożenie	<ol style="list-style-type: none"> Zakres przedmiotu zamówienia obejmuje wykonanie instalacji, uruchomienie, wdrożenie oraz konfigurację systemów/licencji zgodnie z wymaganiami Zamawiającego lub najlepszymi praktykami oraz doświadczeniem Dostawcy. Ponadto, Dostawca zobowiązuje się do przeprowadzenia szkolenia dla co najmniej jednego pracownika Zamawiającego w zakresie obsługi systemów/licencji przy czym ukończenie szkolenia zostanie potwierdzone odpowiednim certyfikatem lub zaświadczeniem Oprogramowanie systemowe musi być zainstalowane <p>Wdrożenie musi zostać przeprowadzone przez Producenta systemu w siedzibie zamawiającego i zawierać:</p> <ol style="list-style-type: none"> Analizę wymagań: <ul style="list-style-type: none"> Wdrożenie ma zawierać szczegółową analizę potrzeb firmy, obejmującą środowisko IT, wymagania w zakresie ochrony danych oraz procesy biznesowe. Określenie, jakie systemy i dane będą podlegały backupowi i archiwizacji oraz jakie mechanizmy bezpieczeństwa są wymagane. Projektowanie architektury rozwiązania: Opracowanie planu wdrożenia, w tym zaprojektowanie architektury systemu backupowego, który będzie odpowiadał na potrzeby organizacji. Dostosowanie rozwiązań oprogramowania do specyfiki IT, w tym integracja z chmurą, wirtualizacją i systemami operacyjnymi. Implementacja i konfiguracja: 	SPEŁNIA TAK / NIE



		<ul style="list-style-type: none"> • Zainstalowanie i skonfigurowanie oprogramowania na serwerach, stacjach roboczych i urządzeniach mobilnych. • Dostosowanie ustawień do wymagań zamawiającego, takich jak harmonogramy kopii zapasowych, zasady retencji danych czy poziom ochrony danych. <p>4. Testowanie i walidacja:</p> <ul style="list-style-type: none"> • Przeprowadzenie testów, aby upewnić się, że system działa zgodnie z oczekiwaniami. • Testowanie procesu odzyskiwania danych, aby sprawdzić, czy dane można szybko i skutecznie przywrócić w razie awarii. <p>5. Szkolenie użytkowników końcowych i administratorów:</p> <ul style="list-style-type: none"> • Szkolenie pracowników odpowiedzialnych za zarządzanie systemem backupowym, w tym administratorów IT i innych użytkowników końcowych. 	
28	Elementy montażowe	Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych	SPEŁNIA TAK / NIE
29	Oświadczenia i certyfikaty	<p>Oświadczenie Producenta oprogramowania wymienionego w pkt. 11 niniejszej specyfikacji technicznej sprzętu potwierdzające, że serwis (opieka techniczna) będzie świadczona przez Producenta i Wykonawcę. Dokument należy złożyć wraz z ofertą.</p> <p>Ponadto producent poświadczy, iż Wykonawca jest autoryzowanym partnerem i posiada należyte kompetencje do wykonania i przeprowadzenia wdrożenia wraz ze szkoleniem dla zaproponowanego rozwiązania. Dokument należy złożyć wraz z ofertą.</p>	SPEŁNIA TAK / NIE



KOD CPV - 32420000-3 - Urządzenia sieciowe

III. Urządzenie Acces Point- 4 sztuki

L.P	Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry
1	Acces point	Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.	<p>SPEŁNIA TAK / NIE</p> <p>Producent</p> <p>Model wersja</p>
2	Płyta główna	<ol style="list-style-type: none"> Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych: <ol style="list-style-type: none"> Temperatura -20 – 45°C, Wilgotność 5–90%. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażona w złącze typu Kensington. Urządzenie musi być wyposażone w dwa niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy: <ol style="list-style-type: none"> 2.4 GHz 802.11b/g/n, 5 GHz 802.11a/n/ac. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 16 SSID. Urządzenie musi być wyposażone w moduł BLE. Urządzenie musi być wyposażone w jeden interfejs 10/100/1000 Base-TX. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3af lub zewnętrzny zasilacz. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych: <ol style="list-style-type: none"> Tunnel, Bridge, Mesh. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA-PSK, WPA-TKIP, WPA2-AES, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA). 	<p>SPEŁNIA TAK / NIE</p>



		<p>11. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:</p> <ol style="list-style-type: none"> MIMO – 2x2, Maksymalna przepustowość dla poszczególnych modułów radiowych: <ul style="list-style-type: none"> 400 Mbps; 867 Mbps; Wymagana moc nadawania: <ul style="list-style-type: none"> min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm; min. 24 dBm dla pasma 5GHz z możliwością zmiany co 1dBm; Wsparcie dla 802.11n 20/40Mhz HT, Wsparcie dla kanałów 80MHz, Anteny – 4 wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy, Maksymalna deklarowana liczba klientów per moduł radiowy: <ul style="list-style-type: none"> 512; 512; <p>12. Funkcje dodatkowe:</p> <ol style="list-style-type: none"> 802.11ac MU-MIMO Wave 2 Transmit Beam Forming (TxBF) Low-Density Parity Check (LDPC) Encoding Maximum Likelihood Demodulation (MLD) Maximum Ratio Combining (MRC) A-MPDU and A-MSDU Packet Aggregation 	
3	Gwarancja, wdrożenie oraz wsparcie	<ul style="list-style-type: none"> Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres do 30.06. 2026 r., polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. Dla zapewnienia wysokiego poziomu usług, świadczenie wsparcia technicznego oraz wdrożenie rozwiązania musi być realizowane przez certyfikowanego inżyniera, posiadającego minimum 4 aktywne certyfikaty. Nie dopuszcza się łączenia certyfikatów przez dwóch lub więcej inżynierów ze względu na poziom bezpieczeństwa oferowanej usługi. (dołączyć do oferty) <p>a) Certyfikowany Specjalista w zakresie Bezpieczeństwa Sieci(NS) (dołączyć do oferty) b) Certyfikowany Specjalista w zakresie Operacji Bezpieczeństwa(SO) (dołączyć do oferty) c) Certyfikowany Specjalista w zakresie Dostępu Zero Trust(ZTA) (dołączyć do oferty) d) Certyfikowany Specjalista w zakresie Bezpieczeństwa Chmury Publicznej(PCS) (dołączyć do oferty)</p>	SPEŁNIA TAK / NIE



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Cyberbezpieczny
Samorząd

Uwaga: Prawą stronę tabeli, należy wypełnić stosując słowa „spełnia” lub „nie spełnia”, zaś w przypadku wyższych wartości niż minimalne-wykazane w tabeli należy wpisać oferowane wartości techniczno-użytkowe. W przypadku, gdy Wykonawca w którejkolwiek z pozycji wpisze słowa „nie spełnia” lub zaoferuje niższe wartości oferta zostanie odrzucona, gdyż jej treść nie odpowiada treści SWZ. Wypełnienie stanowi potwierdzenie zgodności oferowanego sprzętu z wymaganiami Zamawiającego.

INFORMACJE DODATKOWE:

1. W specyfikacji technicznej oferowanego sprzętu i oprogramowania należy **wypełnić każdy wiersz każdej tabeli**. Wykonawca zobowiązany jest także podać m.in. model lub typ urządzenia/nazwę i wersję oprogramowania, nazwę producenta. Zaoferowany przez Wykonawcę sprzęt i oprogramowanie powinien spełniać poszczególne wymagania w zakresie wskazanym w tabeli.
2. Wszędzie tam, gdzie przedmiot zamówienia jest opisany poprzez odniesienie do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa art. 101 ust.1 pkt 2 i ust.3 ustawy prawo zamówień publicznych, Zamawiający dopuszcza zastosowanie przez Wykonawcę rozwiązań równoważnych w stosunku do opisanych w niniejszym SWZ, pod warunkiem, że będą one posiadały co najmniej takie same lub lepsze parametry jakościowe, techniczne i funkcjonalne i nie obniżą określonych standardów.
3. Nazwy własne użyte w SWZ są tylko przykładami pożądanej przez Zamawiającego konfiguracji produktów, które spełniają wymogi Zamawiającego i będą zgodne z użytkowanym sprzętem oraz oprogramowaniem.
4. Wykonawca, który powołuje się na rozwiązania równoważne z opisanymi przez Zamawiającego w niniejszym SWZ, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone (opisane) przez Zamawiającego. Równoważność pod względem parametrów technicznych, użytkowych oraz eksploatacyjnych ma w szczególności zapewnić uzyskanie parametrów technicznych nie gorszych od założonych w niniejszej SWZ.
5. W przypadku, gdy Wykonawca zaproponuje w ofercie produkt równoważny, to w specyfikacji technicznej oferowanego sprzętu musi zawrzeć nazwę produktu (typ, producenta), oraz dokładny opis techniczny oferowanego produktu równoważnego z podaniem jego parametrów technicznych.
6. Wykonawcy mogą składać oferty równoważne w stosunku do przedmiotu zamówienia przedstawionego w SWZ co oznacza, że Zamawiający dopuszcza dostawę sprzętu i oprogramowania równoważnego, jednakże zastrzega sobie prawo do przeprowadzenia testów kompatybilności z istniejącym sprzętem oraz oprogramowaniem. Testy kompatybilności zostaną przeprowadzone na sprzęcie dostarczonym przez Wykonawcę i na jego koszt.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Cyberbezpieczny
Samorząd

7. Wykonawca zobowiązuje się dostarczyć urządzenia do testów w terminie do 72 godzin od wezwania przez Zamawiającego.
8. Równoważność rozwiązań zostanie oceniona na etapie badania złożonych ofert.
9. Zamawiający nie dopuszcza oferowania sprzętów powystawowych.
10. Koszt dostawy wraz z wniesieniem na miejsce wskazane przez Zamawiającego pokrywa we własnym zakresie Wykonawca.
11. Wykonawca dostarczy oraz przekaze pracownikowi dokonującemu odbioru ze strony Zamawiającego sprzęt w oryginalnym opakowaniu wraz z licencjami, dokumentacją użytkową, gwarancją, płytami instalacyjnymi, sterownikami, certyfikatami itp.
12. Zaoferowany sprzęt, a także oprogramowanie muszą być fabrycznie nowe, wolne od wad fizycznych i prawnych, dostarczone w oryginalnych opakowaniach fabrycznych producenta, dostarczone wraz z kompletem standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej, zgodne z odpowiednimi normami i innymi wymaganiami formalnymi, objęte gwarancją i muszą pochodzić z legalnego kanału sprzedaży na rynek Unii Europejskiej.

DOKUMENT POWINIEN BYĆ PODPISANY ELEKTRONICZNIE PRZEZ OSOBĘ UPRAWNIONĄ DO REPREZENTOWANIA WYKONAWCY LUB OSOBĘ UPOWAŻNIONĄ DO WYSTĘPOWANIA W JEGO IMIENIU