Nr sprawy: **OA.271.1.2026.ŁC**

Załącznik Nr 1 do Zapytania ofertowego

...................................................... data ………..

pieczęć firmowa Wykonawcy

1. **FORMULARZ OFERTOWY**
2. **W RAMACH PROJEKTU GRANTOWEGO**
3. **DOT. ZAPYTANIA OFERTOWEGO Z DNIA 23.01.2026r. OA.271.1.2026**

**WYKONAWCA:**

Nazwa:………………………………………………………………………………………………….

Adres Wykonawcy: …………………………………………………………………………………….

Nr telefonu: …………………………………………………………………………………………….

E-mail: ………………………………………………………………….………………………………

NIP: ……………………………………REGON:……………………………………………………..

W nawiązaniu do zapytania ofertowego składam ofertę w postępowaniu prowadzonym zgodnie z Zasadą konkurencyjności, którego przedmiotem jest projekt grantowy „Cyberbezpieczny Samorząd dla Gminy Miasto Wąbrzeźno” na potrzeby działania Gminy Miasto Wąbrzeźno w ramach programu FERC 2021-2027, oś priorytetowa II: Zaawansowane usługi cyfrowe, Działanie 2.2., wzmocnienie krajowego systemu cyberbezpieczeństwa. za cenę ofertową:

**Wykonanie zadania – Cyberbezpieczny Samorząd – Gmina Miasto Wąbrzeźno”**

**Oferuję wykonanie zamówienia – dostawa serwera, za cenę łączną brutto w wysokości: …………………………. zł**

**słownie: …………………………………………………………………………………………………….……**

w tym kwota netto …………............................................................................................................................ zł

słownie: ..................................................................................................................................................................

podatek VAT w wysokości ……………….... % tj. …….………………………………..…………………zł

słownie: .................................................................................................................................................................

**w terminie: ……….. dni od podpisania umowy**

1. Oferuję/emy wykonanie dostaw i usług objętych zamówieniem zgodnie z wymogami zapytania ofertowego.
2. **Oświadczam/ oświadczamy, że:**

* zapoznałem się z warunkami zamówienia i przyjmuję je bez zastrzeżeń;
* zapoznałem się z postanowieniami załączonego do zapytania ofertowego wzoru umowy i przyjmuję go bez zastrzeżeń;
* oświadczam/y, że wzór umowy stanowiący odpowiednio załącznik nr 5a dla części 1 oraz 5b dla części 2 do zapytania ofertowego został przez nas zaakceptowany i zobowiązujemy się w przypadku wyboru naszej oferty do zawarcia umowy na warunkach w nim określonych, w miejscu i terminie wyznaczonym przez Zamawiającego.
* przedmiot oferty jest zgodny z przedmiotem zamówienia;
* zrealizuję zamówienie w terminie wskazanym w zapytaniu ofertowym,
* jestem związany z niniejszą ofertą przez okres 30 dni, licząc od dnia składania ofert podanego w zapytaniu ofertowym,
* gwarantujemy stałość cen przez cały okres trwania umowy,
* w cenie wskazanej w niniejszej ofercie wliczone są wszystkie niezbędne składniki do realizacji zamówienia,
* wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO [rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1)\*] wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.\*\*

UWAGA:

*(\*) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1).*

*(\*\*)w przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie).*

1. **Osobą do kontaktu w sprawie złożonej oferty jest:**

Imię i nazwisko …………………………..……………….

Stanowisko: ……………………………….…...................

Tel …………………………………..……………………

e-mail: ……………………………..……………………

1. **Rodzaj przedsiębiorstwa, jakim jest Wykonawca** *(proszę zaznaczyć właściwą opcję)*

* **Mikroprzedsiębiorstwo**
* **Małe przedsiębiorstwo**
* **Średnie przedsiębiorstwo**

*W przypadku Wykonawców składających ofertę wspólną należy wypełnić dla każdego podmiotu osobno.*

*Mikroprzedsiębiorstwo: przedsiębiorstwo, które zatrudnia mniej niż 10 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 2 milionów EURO.*

*Małe przedsiębiorstwo: przedsiębiorstwo, które zatrudnia mniej niż 50 osób i katorgo roczny obrót lub roczna suma bilansowa nie przekracza 10 milionów EURO.*

*Średnie przedsiębiorstwo: przedsiębiorstwo, które nie jest mikro przedsiębiorstwem ani małym przedsiębiorstwem i które zatrudnia mniej niż 250 osób i którego roczny obrót nie przekracza 50 milionów EUR. lub roczna suma bilansowa nie przekracza 43 milionów EURO.*

**6.** Oświadczam, że przedmiot zamówienia wykonam osobiście/z udziałem podwykonawcy/ów.\*

Informuję, że zamierzam powierzyć następujące realizację zamówienia Podwykonawcom:

............................................................................................................................................................................  
*/zakres/*

Firmy (nazwy) Podwykonawców: …………………………………….……………………………………...

*/o ile nazwy podwykonawców są dla wykonawcy znane na czas składania oferty/*

Łączna wartość dostaw wykonanych przez Podwykonawców stanowić będzie kwotę ……………..…. zł, tj. …. % wartości całego zamówienia.

7. **Zastrzeżenie tajemnicy przedsiębiorstwa**

Oświadczam/y, że informacje i dokumenty zawarte w Ofercie na stronach od nr ........................ do nr ......................... stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji i zastrzegamy, że nie mogą być one udostępniane. Informacje i dokumenty zawarte na pozostałych stronach Oferty są jawne.

*(W przypadku utajnienia oferty Wykonawca zobowiązany jest wykazać, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa w szczególności określając, w jaki sposób zostały spełnione przesłanki, o których mowa w art. 11 pkt. 2 ustawy z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji).*

8. Jesteśmy świadomi odpowiedzialności karnej za złożenie fałszywego oświadczenia.

1. **Załącznikami do niniejszej oferty są:**

1) ……………………………………………………………………………………………

2) ……………………………………………………………………………………………

3) ……………………………………………………………………………………………

4) ……………………………………………………………………………………………

......................................, dnia …….........................

….……...…………………………………

*Podpis osób uprawnionych do składania*

*oświadczeń woli w imieniu Wykonawcy oraz pieczątka / pieczątki*

**Wykaz parametrów technicznych oferowanego sprzętu – niezbędny załącznik do cz. 1 – dostawa serwera**

1. **Serwer do wirtualizacji**

Serwer

Producent: …………………………………….

Model: …………………………………….

Ilość: 1 szt.

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry techniczne** |
| **Obudowa** | * Obudowa Rack o wysokości max 2U z możliwością instalacji min. 24 dysków 2.5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. * Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. * 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. |  |
| **Płyta główna** | * Płyta główna z możliwością zainstalowania do dwóch procesorów. * Obsługa procesorów 56 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. |  |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |  |
| **Procesor** | Zainstalowane dwa procesory min. 16-rdzeniowe klasy x86, dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 280 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. |  |
| **RAM** | Minimum 128GB DDR5 RDIMM 5600MT/s, |  |
| **Funkcjonalność pamięci RAM** | * Demand Scrubbing, * Patrol Scrubbing, * Permanent Fault Detection (PFD) |  |
| **Gniazda PCI** | Min. 8 slotów PCIe w tym minimum 6 slotów FH |  |
| **Interfejsy sieciowe/FC/SAS** | Wbudowane min. 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) |  |
| **Dyski twarde** | * Zainstalowane:   + 2 x Dysk 1.92 TB (SSD Read Intensive, SAS 24 Gb/s, 2.5″, Hot-Plug) |  |
| **Kontroler RAID** | * Sprzętowy kontroler dyskowy, posiadający   + Min. 8GB nieulotnej pamięci cache,   + Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.   + Wsparcie dla dysków samoszyfrujących |  |
| **Wbudowane porty** | * 4x USB, w tym min. 1 porty USB 3.0 * 2x port VGA (jeden na panelu przednim) * Możliwość rozbudowy o Serial Port |  |
| **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024 |  |
| **Wentylatory** | Redundantne, Hot-Plug |  |
| **Zasilacze** | Redundantne, Hot-Plug min. 1100W klasy Titanium |  |
| **System operacyjny/dodatkowe oprogramowanie** | Licencje wymagane są do zaimplementowania wirtualizacji do infrastruktury zamawiającego.  Licencje na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie czterech instancji wirtualnych tego serwerowego systemu operacyjnego.  Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na zoferowanym serwerze.  Licencje tzw. CAL – dostępowe, per user lub urządzenie obejmujące min. 70 użytkowników lub urządzeń.  Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.  1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.  2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.  3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.  4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.  5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.  6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.  7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.  8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.  9) Wbudowane wsparcie instalacji i pracy na wolumenach, które:  a) pozwalają na zmianę rozmiaru w czasie pracy systemu,  b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,  c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,  d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).  10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.  11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.  12) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET  13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.  14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.  15) Dostępne dwa rodzaje graficznego interfejsu użytkownika:  a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,  b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.  16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,  17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.  18) Mechanizmy logowania w oparciu o:  a) Login i hasło,  b) Karty z certyfikatami (smartcard),  c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),  19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..  20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).  21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.  22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.  23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).  24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.  25) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:  a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,  b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:  I. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  II. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  III. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.  IV. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.  c) Zdalna dystrybucja oprogramowania na stacje robocze.  d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej  e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:  I. Dystrybucję certyfikatów poprzez http  II. Konsolidację CA dla wielu lasów domeny,  III. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,  IV. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.  f) Szyfrowanie plików i folderów.  g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).  h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.  i) Serwis udostępniania stron WWW.  j) Wsparcie dla protokołu IP w wersji 6 (IPv6),  k) Wsparcie dla algorytmów Suite B (RFC 4869),  l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,  m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:  I. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  II. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.  III. Obsługi 4-KB sektorów dysków  IV. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra  V. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.  VI. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)  26) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.  27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).  28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.  29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.  30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. |  |
| **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * Możliwość wyłączenia w BIOS funkcji przycisku zasilania. * BIOS 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 |  |
| **Moduł bezpieczeństwa** | Zainstalowany fabrycznie w urządzeniu na złączu PCIe v2 lub v3 sprzętowy moduł bezpieczeństwa umożliwiający bezpieczne przechowywanie kluczy kryptograficznych oraz wspierający operacje kryptograficzne z użyciem kluczy asymetrycznych RSA długości nie mniejszej niż 8192bitów, Diffie-Helmana oraz ECC Suite B. Moduł musi posiadać wsparcie dla algorytmów symetrycznych AES o długości nie mniejszej niż 256bit oraz 3 (Triple) DES 112 i 168 bitów. Obsługę funkcji skrótu SHA-1 i SHA-2 o długości (224, 256, 284 oraz 512 bitów). Moduł bezpieczeństwa musi posiadać certyfikację FIPS 140-2 poziomu 3 (certyfikat należy załączyć do oferty), oraz umożliwiać pełne zdalne zarządzanie włącznie z aktualizacją firmware. Dodatkowo moduł ten musi pozwalać na autoryzację za pomocą hasła, karty inteligentnej (która musi zostać dostarczona wraz urządzeniem, i dedykowanym czytnikiem współpracującym tylko z kartami danego producenta) oraz klucza w postaci pliku. Wraz z modułem kryptograficznym musi zostać dostarczone oprogramowanie producenta modułu będące odpowiednikiem zaoferowanego fizycznego modułu bezpieczeństwa. Moduł bezpieczeństwa musi oferować zaawansowaną diagnostykę i logowanie zdarzeń w przynajmniej 3 poziomach (Error, Warning, Info), przy wykorzystywaniu biblioteki PKCS#11. |  |
| **Karta Zarządzania** | * Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   + zdalny dostęp do graficznego interfejsu Web karty zarządzającej;   + zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);   + szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;   + możliwość podmontowania zdalnych wirtualnych napędów;   + wirtualną konsolę z dostępem do myszy, klawiatury;   + wsparcie dla IPv6;   + wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;   + możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;   + możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;   + integracja z Active Directory;   + możliwość obsługi przez dwóch administratorów jednocześnie;   + wsparcie dla dynamic DNS;   + wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.   + możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera   + możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera   oraz z możliwością rozszerzenia funkcjonalności o:   * + Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej   + Przesyłanie danych telemetrycznych w czasie rzeczywistym   + Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze   + Automatyczna rejestracja certyfikatów (ACE) |  |
| **Oprogramowanie do zarządzania** | * Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:   + 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   + 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 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. |  |
| **Certyfikaty** | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 * Serwer musi posiadać deklaracja CE. * Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami – załączyć do ofert dokumentację techniczną lub oświadczenie producenta serwera w celu potwierdzenia spełnienia normy * 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](http://www.epeat.net) potwierdzający spełnienie normy co najmniej Epeat Silver 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 2019, Microsoft Windows Server 2022. |  |
| **Dokumentacja użytkownika** | * Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim. * Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |  |
| **Warunki gwarancji** | * Zamawiający wymaga zapewnienia przez wykonawcę usługi wsparcia technicznego z zakresu wdrażanej technologii na okres 3 lat. * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. * Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy (dla krytycznych zgłoszeń serwisowych) * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. * Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / 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. * Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. * 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 wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. * 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. * Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. |  |

….……...…………………………………

*Podpis osób uprawnionych do składania*

*oświadczeń woli w imieniu Wykonawcy oraz pieczątka / pieczątki*