Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

**ZAŁĄCZNIK NR 4A DO SWZ**

**OŚWIADCZENIE SKŁADANE WRAZ Z OFERTĄ  
(PRZEDMIOTOWY ŚRODEK DOWODOWY)**

**Nazwa Wykonawcy:**

|  |
| --- |
|  |

**Oświadczenie**

**dot. potwierdzenia parametrów technicznych oferowanego sprzętu komputerowego z minimalnymi wymagania Zamawiającego, składane w postępowaniu o udzielenie zamówienia publicznego pod nazwą: Zakup niezbędnego sprzętu, wyposażenia, oprogramowania (obszar techniczny) na potrzeby Urzędu Miasta Zgorzelec w ramach projektu pn. "Cyberbezpieczny Urząd Miasta Zgorzelec".**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **TABELA A – serwer rack** | | |
| Lp. | Nazwa komponentu | Minimalne wymagania techniczne serwera | Oferowane parametry przez Wykonawcę  (\*niepotrzebne skreślić lub usunąć) |
| **1** | **2** | **3** | **4** |
| 1. | Typ | Serwer rack | Producent: |
| Model: |
| 2. | Obudowa | Obudowa Rack o wysokości max 1U | Tak/nie\* |
| Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy,   * Identyfikacja stanu serwera * Wyświetlanie podstawowych stanów działania serweraw tym adres IP karty zarządzającej | Tak/nie\* |
| 3. | Płyta główna | -Płyta główna z możliwością zainstalowania do dwóch fizycznych procesorów.  -Obsługa procesorów 56 rdzeniowych.  -Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.  -Na płycie głównej powinny znajdować się minimum 32 sloty przeznaczone do instalacji pamięci.  -Płyta główna powinna obsługiwać do 8TB pamięci RAM | Tak/nie\* |
| 4. | Chipset | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych | Tak/nie\* |
| 5. | Procesor | Zainstalowane dwa procesory z fizycznymi 16 rdzeniami, klasy x86 dedykowane do pracy z zaoferowanym serwerem, osiągające wydajność minimum **34380** pkt każdy w teście Passmark- CPU Mark – Server CPU Performance  <https://www.cpubenchmark.net/server.html>  na dzień 25.02.2025  Testy w załączeniu – **Tabela A2**  lub  Umożliwiające osiągnięcie wyniku min. 266 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. | Model: |
| 6. | Pamięć RAM | Minimum 256GB DDR5 RDIMM 5600MT/s, | Wielkość: |
| 7. | Karta graficzna | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 | Model: |
| 8. | Pamięć masowa | Zainstalowane **dwa** dyski M.2 NVMe SSD o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. | Wielkość dysku: |
| 9. | Gniazda PCI | Trzy sloty PCIe LP | Tak/nie\* |
| 10. | 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) * Dwuportowa karta sieciowa 25Gb Ethernet w standardzie SFP28 | Tak/nie\* |
| 11. | Porty i złącza | * 4 porty USB w tym min:   + 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 | Tak/nie\* |
| 12. | Zasilacze | Dwa Redundantne, Hot-Plug min. 1100W klasy Titanium | Tak/nie\* |
| 13. | Elementy montażowe | * Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych * Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych | Tak/nie\* |
| 14. | System operacyjny | Windows Server 2025 Standard PL– licencja dobrana tak aby przy oferowanych procesorach umożliwić uruchomienie 4 nowych maszyn wirtualnych ( dopuszczalna wersja systemu operacyjnego związana ze sprzętem- licencja typu ROK-Reseller Option Kit), **lub równoważny wg Tabeli A1** | Nazwa systemu:  Ilość licencji : |
| 15. | Licencje dostępowe | 120 licencji Windows Server 2025/2022 User CAL (dopuszczalne zestawy grupowe licencji) | Tak/nie\* |
| 16. | Bezpieczeństwo | * Zatrzask 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 V3 * 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). | Tak/nie\* |
| 17. | 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 automatycznej rejestracji 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) | Tak/nie\* |
| 18. | 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. | Tak/nie\* |
| 19. | Oprogramowanie do monitorowania | Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:   * Monitoring:   + 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:     - 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:     - 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:     - 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   + 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   + Możliwość generowania raportów dla serwerów zawierających informację o:     - 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:     - 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   + 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   + Urządzenie Producenta dostarczane  w ramach postępowania   + Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatorów Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) * Wirtualny asystent   + 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   + Możliwość rozbudowy systemu  o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT.   Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android | Tak/nie\* |
| 20. | Certyfikaty  i standardy | * 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](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 2022.  Ww. dokumenty należy dostarczyć Zamawiającemu wraz ze sprzętem komputerowym | Tak/nie\* |
| 21. | 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. | Tak/nie\* |
| 22. | Warunki gwarancji | * Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. * Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. * Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. * Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. * Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych  i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części,  a także ocena bezpieczeństwa cybernetycznego. * Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:   + 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. * Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.   Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.  (oświadczenie należy dostarczyć Zamawiającemu wraz ze sprzętem komputerowym). | Tak/nie\* |

**UWAGA!  
\* Kolumna nr 4 - do wypełnienia przez Wykonawcę. Wykonawca może zaoferować parametry wyższe od minimalnych wymaganych przez Zamawiającego (kolumna nr 3) lub równoważne, nie gorsze niż określone przez Zamawiającego.**Zamawiający wymaga wypełnienia ww. kolumny w sposób niżej określony:

1. Pozycje nr 1, 5-8, 14 – należy wpisać konkretne parametry oferowanego serwera,
2. Pozycje nr 2-4, 9–13, 15-22 – należy zaznaczyć odpowiedź „TAK lub NIE”.

Brak w ofercie jednoznacznego wskazania wymaganego parametru lub potwierdzenia parametru – zgodnie z ww. zapisami i/lub zmiana opisów pozycji, spowoduje odrzucenie oferty na podstawie art. 226 ust. 1 pkt. 5) ustawy Pzp jako oferty, której treść jest niezgodna z warunkami zamówienia.

**W przypadku rozwiązań równoważnych należy uzupełnić tabelę A1.**

|  |  |  |
| --- | --- | --- |
| **TABELA A1  UWAGA! Tabelę należy wypełnić w przypadku oferowania produktu równoważnego w stosunku do Tabela A- serwer rack, pozycja „System operacyjny”:** | | |
|  | W przypadku zaoferowania przez Wykonawcę licencji systemu równoważnego do systemu Microsoft Windows Server 2022/2025 , Zamawiający wymaga dostarczenia odpowiedniej ilości licencji dla serwera fizycznego oraz serwerów wirtualnych, oraz instalację i migrację obecnego środowiska. Zamawiający wymaga aby produkt równoważny spełniał niżej wymienione wymagania:   1. Współpraca z procesorami o architekturze x86 – 64bit. 2. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym. 3. Możliwość budowania klastrów składających się z 64 węzłów. 4. Licencja/licencje muszą obsłużyć serwer fizyczny wyposażony w zaproponowane procesory / fizyczne rdzenie. 5. Praca w roli klienta domeny Microsoft Active Directory. 6. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie funkcjonalności Microsoft Windows Server 2019. 7. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu. 8. Możliwość uruchomienia roli klienta i serwera czasu (NTP). 9. Możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory. 10. Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory. 11. Możliwość uruchomienia roli serwera stron WWW. 12. W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera. 13. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego. 14. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów). 15. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 16. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. 17. Wbudowane wsparcie instalacji i pracy na wolumenach, które:     1. pozwalają na zmianę rozmiaru w czasie pracy systemu,     2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,     3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,     4. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 18. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość 19. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 20. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET 21. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 22. Możliwość wykorzystania standardu http/2. 23. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 24. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe. 25. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 26. Mechanizmy logowania w oparciu o: a) login i hasło,     1. karty z certyfikatami (smartcard),     2. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM). 27. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:     1. określonych grup użytkowników,     2. zastosowanej klasyfikacji danych,     3. centralnych polityk dostępu w sieci,     4. centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. 28. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 29. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 30. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 31. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 32. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 33. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:     1. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.     2. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:        * + podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,          + ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,          + odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,          + bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.,     3. zdalna dystrybucja oprogramowania na stacje robocze,     4. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników,     5. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:        * + Dystrybucję certyfikatów poprzez http,          + Konsolidację CA dla wielu lasów domeny,          + Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,          + Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.     6. szyfrowanie plików i folderów,     7. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),     8. szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi,     9. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,     10. serwis udostępniania stron WWW,     11. wsparcie dla protokołu IP w wersji 6 (IPv6),     12. wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,     13. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie uruchomienie nieograniczonej liczby aktywnych środowisk wirtualnych systemów operacyjnych (liczba ograniczona parametrami fizycznymi serwera),     14. możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.     15. możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.     16. mechanizmy wirtualizacji mające wsparcie dla:         * + dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,           + obsługi ramek typu jumbo frames dla maszyn wirtualnych.           + obsługi 4-KB sektorów dysków,           + nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,           + możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.     17. możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.     18. wsparcie dla rozwiązania Kubernetes.     19. 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.     20. wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).     21. mechanizmy deduplikacji i kompresji na wolumenach.     22. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.     23. mechanizm konfiguracji połączenia VPN do platformy Azure.     24. wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.     25. mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.     26. możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL )Server Standard). |  |
| Zapewniający pełną kompatybilność z istniejąca infrastrukturą Zamawiającego, a w szczególności z posiadanym oprogramowaniem  -praca jako stacje końcowe PC | w pełni kompatybilny z posiadanym oprogramowaniem Zamawiającego, pozwalający uruchamiać poniższe oprogramowanie bezpośrednio z poziomu systemu operacyjnego, bez dodatkowego oprogramowania (emulatora) lub warstwy wirtualizacyjnej :  **Do każdego poniższego oprogramowania wymagane oświadczenie producenta** oprogramowania o zgodności z proponowanym systemem operacyjnym (oświadczenie należy dostarczyć Zamawiającemu wraz ze sprzętem komputerowym).   1. system finansowo-księgowy ZSI SIGID (https://sigid.pl/) 2. system sprawozdawczości Besti@ (<https://budzetjst.pl/>) 3. Rejestr Zaangażowania Środków Budżetowych-Doskomp (https://portal.jst.pl/) 4. Legislator (<https://www.abcpro.pl/eap-legislator>) 5. Axence nVision 6. Eset XDR |  |

**Niniejszy dokument należy opatrzyć kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym.   
Uwaga! Nanoszenie jakichkolwiek zmian w treści dokumentu po opatrzeniu ww. podpisem może skutkować naruszeniem integralności podpisu, a w konsekwencji skutkować odrzuceniem oferty.**Zamawiający zaleca przed podpisaniem, zapisanie dokumentu   
w formacie .pdf